

**Vysoká škola báňská – Technická univerzita Ostrava**  
**Fakulta elektrotechniky a informatiky**  
**Katedra telekomunikačnej techniky**

**Nasadenie monitorovacieho nástroja HOMER**  
**Deployment of HOMER-based Monitoring System**

**2018**

**Patrik Nechajev**

VŠB - Technická univerzita Ostrava  
Fakulta elektrotechniky a informatiky  
Katedra telekomunikační techniky

## Zadání bakalářské práce

Student:

**Patrik Nechajev**

Studijní program:

B2647 Informační a komunikační technologie

Studijní obor:

2601R013 Telekomunikační technika

Téma:

Nasazení monitorovacího nástroje HOMER  
Deployment of HOMER-based Monitoring System

Jazyk vypracování:

čeština

Zásady pro vypracování:

HOMER 5 je pokročilý monitorovací systém určený pro sledování a vyhodnocování probíhající SIP signalizace, který umožňuje nasazení i v provozech s objemnými toky signalizačních dat.

Práce sestává z následujících bodů:

1. Student si nastuduje a popíše monitorovací nástroj HOMER, jeho účel, využitelnost i možnosti propojení s dalšími SIP systémy.
2. Student navrhne a realizuje testovací prostředí pro zjištění možností monitorovacího systému HOMER a pro ověření věrohodnosti zobrazovaných dat.
3. Student provede zátěžový test navrženého systému.
4. Student zhodnotí monitorovací nástroj HOMER z pohledu jeho využitelnosti v praktickém nasazení, přesnost prezentovaných výsledků i rychlost aktualizace prezentovaných dat.

Seznam doporučené odborné literatury:

- [1] Hartpence, B. Packet Guide to Voice over IP: A system administrator's guide to VoIP technologies. ISBN 1449339670.  
[2] Interní dokumentace projektu HOMER - viz <https://github.com/sipcapture/homer>.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Jan Rozhon, Ph.D.**

Datum zadání: 01.09.2017

Datum odevzdání: 30.04.2018

doc. Ing. Miroslav Vozňák, Ph.D.  
vedoucí katedry

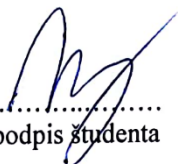


prof. Ing. Pavel Brandštetter, CSc.  
děkan fakulty

## Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne. Uviedol som všetky zdroje informácií a použitú literatúru, z ktorých som čerpal.

V Ostrave dňa: 26. dubna 2018

  
.....  
podpis študenta

## **Pod'akovanie**

Rád by som poďakoval vedúcemu bakalárskej práce Ing. Janovi Rozhonovi, Ph.D. za odbornú pomoc a konzultácie pri vytváraní tejto bakalárskej práce.

Ďalej by som chcel poďakovať svojej rodine a priateľke za to, že ma počas celého štúdia podporovali.

## **Abstrakt**

Táto bakalárska práca je zameraná na spojaznenie, sledovanie a vyhodnocovanie prebiehajúcej SIP signalizácie pomocou monitorovacieho systému HOMER 5.

Dôraz je kladený na inštaláciu systému HOMER 5, jeho účel, možnosti využiteľnosti a analýzy dát. Ďalej bude nasledovať spojazdnenie systému HOMER 5, ktorý pripojím na môj Asterisk server, komunikáciu bude riadiť SIP protokol. Potom sa budem venovať navrhnutiu testovacieho prostredia, ktoré bude slúžiť k analýze, overeniu dôveryhodnosti a k záťažovému testu navrhnutého systému.

Samotné testovanie je vykonané pomocou nástroja SIPp, ktorý je určený k testovaniu SIP protokolu. V práci som vykonal overenie za účelom dôveryhodnosti prezentovaných dát pomocou nástroja Wireshark.

## **Kľúčové slová**

Asterisk; HOMER; Linux; PJSIP; SIP; SIPp; VoIP

## **Abstract**

This bachelor thesis is focused on monitoring and evaluation of ongoing SIP signaling using the HOMER 5 monitoring system.

Emphasis is put on installing the HOMER 5, its purpose, possibilities of use and data analysis. Next the HOMER 5 will be connected with Asterisk PBX, communication will be handled by SIP protocol. Then I will give the effort to designing a test environment, which serves to data analysis, to verify trustworthiness and to stress test of the system.

Testing itself is executed with SIPp testing tool used for testing of SIP protocol. In thesis I have done the verification of the presented data with the help of the Wireshark tool.

## **Key words**

Asterisk; HOMER; Linux; PJSIP; SIP; SIPp;VoIP

## Zoznam použitých skratiek

| Skratka     | Význam                                     |
|-------------|--|
| <b>GPG</b>  | GNU Privacy Guard                          |
| <b>HEP</b>  | Homer Encapsulation Protocol               |
| <b>HTTP</b> | Hypertext Transfer Protocol                |
| <b>IETF</b> | Internet Engineering Task Force            |
| <b>ICE</b>  | Interactive Connectivity Establishment     |
| <b>NAT</b>  | Network Address Translation                |
| <b>OSS</b>  | Open Source Software                       |
| <b>PCAP</b> | Packet Capture                             |
| <b>PSTN</b> | Public Switched Telephone Network          |
| <b>RTP</b>  | Real-Time Transport Protocol               |
| <b>RTCP</b> | Real-Time Control Protocol                 |
| <b>SDP</b>  | Session description Protocol               |
| <b>SIP</b>  | Session Initiation Protocol                |
| <b>STCP</b> | Stream Control Transmission Protocol       |
| <b>STUN</b> | Session Traversal Utilities for NAT        |
| <b>TCP</b>  | Transmission Control Protocol              |
| <b>TURN</b> | Traversal Using Relay NAT                  |
| <b>UDP</b>  | User Datagram Protocol                     |
| <b>VoIP</b> | Voice over the Internet Protocol           |
| <b>XMPP</b> | Extensible Messaging and Presence Protocol |

## Zoznam obrázkov a tabuliek

|  |        |
|--|--------|
| <i>Obrázok 1.1: Porovnanie tradičného telefónu (vľavo) a VoIP systému (vpravo)</i> | - 2 -  |
| <i>Obrázok 1.2: SIP Adresovanie</i>  | - 4 -  |
| <i>Obrázok 1.3: SIP odpoveď na žiadosť o registráciu</i>                           | - 5 -  |
| <i>Obrázok 1.4: Prepojenie medzi sip.conf a extensions.conf</i>                    | - 7 -  |
| <i>Obrázok 1.5: Porovnanie sip.conf a pjsip.conf</i>                               | - 8 -  |
| <i>Obrázok 1.6: Zachytávacie nástroje napojené na HOMER 5</i>                      | - 10 - |
| <i>Obrázok 1.7: Príkazový riadok Asterisku</i>                                     | - 12 - |
| <i>Obrázok 1.8: Overenie správnosti načítania extensions.conf</i>                  | - 15 - |
| <i>Obrázok 1.9: Registrácia účastníka pomocou LinPhone</i>                         | - 15 - |
| <i>Obrázok 2.0: Úspešná inštalácia Docker</i>                                      | - 18 - |
| <i>Obrázok 2.1: Prihlasovacia obrazovka HOMER 5</i>                                | - 19 - |
| <i>Obrázok 2.2: Užívateľské rozhranie HOMER 5</i>                                  | - 20 - |
| <i>Obrázok 2.3: Nakonfigurovaný súbor hep.conf</i>                                 | - 21 - |
| <i>Obrázok 2.4: Úspešné odchytenie HEP paketu pomocou tcpdump</i>                  | - 22 - |
| <i>Obrázok 2.5: Dáta zobrazené v HOMER</i>   | - 23 - |
| <i>Obrázok 2.6: Prepojenie medzi .xml scenárom a .csv súborom</i>                  | - 26 - |
| <i>Obrázok 2.7: Testovacie prostredie</i>  | - 28 - |
| <i>Obrázok 2.8: SIP vyhľadávanie</i>   | - 29 - |
| <i>Obrázok 2.9: Rebríkový diagram hovoru s CallID 2-784@192.168.23.156</i>         | - 29 - |
| <i>Obrázok 3.0: Detaily SIP správy INVITE hovoru s CallID 2-784@192.168.23.156</i> | - 30 - |
| <i>Obrázok 3.1: Štatistika jednotlivých SIP správ</i>                              | - 31 - |
| <i>Obrázok 3.2: Počty paketov jednotlivých testov</i>                              | - 31 - |
| <i>Obrázok 3.3: SIP štatistika jednotlivých testov</i>                             | - 32 - |
| <i>Obrázok 3.4: Veľkosť HEP paketov jednotlivých testov</i>                        | - 32 - |
| <i>Obrázok 3.5: Grafy IP Invites, SIPCapture Packet Count a UAC Invites</i>        | - 33 - |
| <i>Obrázok 3.6: Porovnanie SIP správ v HOMER(hore) a Wireshark(dole)</i>           | - 34 - |
| <i>Obrázok 3.7: Porovnanie rebríkových diagramov</i>                               | - 35 - |
| <i>Obrázok 3.8: Porovnanie SIP hlavičiek v HOMER (vpravo) a Wireshark(vľavo)</i>   | - 35 - |
| <i>Obrázok 3.9: Porovnaní počtu INVITE správ HOMER (vľavo) Wireshark(vpravo)</i>   | - 36 - |
|  |        |
| <i>Tabuľka 1.1: Výpis UAC po dokončení komunikácie</i>                             | - 27 - |
| <i>Tabuľka 1.2: Výpis UAS po dokončení komunikácie</i>                             | - 27 - |
| <i>Tabuľka 1.3: Veľkosť jednotlivých HEP paketov</i>                               | - 33 - |
| <i>Tabuľka 1.4: Tabuľka s výsledkami zo záťažového testu</i>                       | - 37 - |



# Obsah

|  |      |
|--|------|
| Úvod.....  | 1 -  |
| 1 Telefónia cez IP protokol .....                      | 2 -  |
| 1.1 Definícia Voice over the Internet Protocol.....    | 2 -  |
| 1.2 Protokoly využívané vo VoIP .....                  | 2 -  |
| 1.2.1 Signálne protokoly SIP a H.323 .....             | 2 -  |
| 1.2.2 Transportné Protokoly RTP a RTCP .....           | 3 -  |
| 1.3 SIP - Session Initiation Protocol .....            | 3 -  |
| 1.3.1 Komponenty .....                                 | 3 -  |
| 1.3.2 Adresovanie.....                                 | 3 -  |
| 1.3.3 Žiadosti.....                                    | 4 -  |
| 1.3.4 Odpovedi .....                                   | 4 -  |
| 1.3.5 Štruktúra SIP hlavičky.....                      | 5 -  |
| 1.3.6 SDP - Session description Protocol.....          | 5 -  |
| 2 IP Pobočková ústredňa Asterisk v13.....              | 6 -  |
| 2.1 Popis Asterisk.....                                | 6 -  |
| 2.1.1 Podpora protokolu HEP.....                       | 6 -  |
| 2.2 Moduly .....                                       | 6 -  |
| 2.3 Konfigurácia.....                                  | 6 -  |
| 2.4 PJSIP .....  | 7 -  |
| 3 Monitorovací systém HOMER 5.....                     | 9 -  |
| 3.1 Popis monitorovacieho systému .....                | 9 -  |
| 3.2 Komponenty - Capture Server.....                   | 9 -  |
| 3.3 Komponenty - Capture Agents.....                   | 9 -  |
| 3.4 HEP - Homer Encapsulation Protocol.....            | 9 -  |
| 3.5 Možnosti inštalácie.....                           | 10 - |
| 3.5.1 Kontajnerová platforma DOCKER .....              | 11 - |
| 4 Inštalácia a konfigurácia Asterisk .....             | 12 - |
| 4.1 Inštalácia.....                                    | 12 - |
| 4.2 Konfigurácia.....                                  | 13 - |
| 4.3 Registrácia koncových bodov pomocou LinPhone ..... | 15 - |
| 5 Spojazdnenie systému HOMER 5.....                    | 17 - |

|       |   |        |
|-------|---|--------|
| 5.1   | DOCKER - Inštalácia.....                                  | - 17 - |
| 5.2   | Spustenie systému HOMER 5 pomocou platformy DOCKER.....   | - 18 - |
| 5.3   | Užívateľské rozhranie.....                                | - 19 - |
| 5.4   | Prepojenie HOMER 5 a Asterisk pomocou HEP protokolu ..... | - 20 - |
| 6     | Testovací nástroj SIPp.....                               | - 24 - |
| 6.1   | Inštalácia.....   | - 24 - |
| 6.2   | Konfigurácia.....   | - 25 - |
| 7     | Analýza dát.....  | - 28 - |
| 7.1   | HOMER 5 - Analýza dát.....                                | - 28 - |
| 7.2   | Overenie dôveryhodnosti získaných dát.....                | - 34 - |
| 7.2.1 | Porovnanie dát pomocou nástroja Wireshark.....            | - 34 - |
| 8     | Zaťažový test navrhnutého systému.....                    | - 37 - |
|       | Záver .....   | - 39 - |
|       | Použitá literatúra .....                                  | - 40 - |
|       | Elektronické prílohy.....                                 | - 42 - |

# Úvod

Prvá časť bakalárskej práce bude venovaná teórii, konkrétne technológii VoIP a objasnenie na čo slúži. Objasnenie pojmov, ktoré súvisia s VoIP, teda protokoly, hlavne SIP signálny protokol, jeho popis a funkcie ktoré vykonáva.

Ďalej sa budem zaoberať softwarovou pobočkovou ústredňou Asterisk, ktorú budem využívať v tejto práci. Konkrétne využitými modulmi, konfiguráciou a inštaláciou.

Druhou a hlavnou časťou je popis a spoznanie systému HOMER 5 pomocou kontajnerovej platformy DOCKER, prepojenie pomocou HEP protokolu s Asterisk PBX. Následné navrhnutie testovacieho prostredia pomocou PJSIP, ktoré bude slúžiť na zadenovanie koncových bodov. Po navrhnutí testovacieho prostredia rôznymi testami zistím možnosti analýzy dát a celkové možnosti systému HOMER 5.

Ako testovací nástroj využijem nástroj SIPp, ktorý bude využitý k testovaniu navrhnutého prostredia a aj k vykonaniu záťažového testu.

Pre overenie dôveryhodnosti zobrazených dát som zvolil porovnanie zobrazovaných dát s analyzátorom paketov Wireshark.

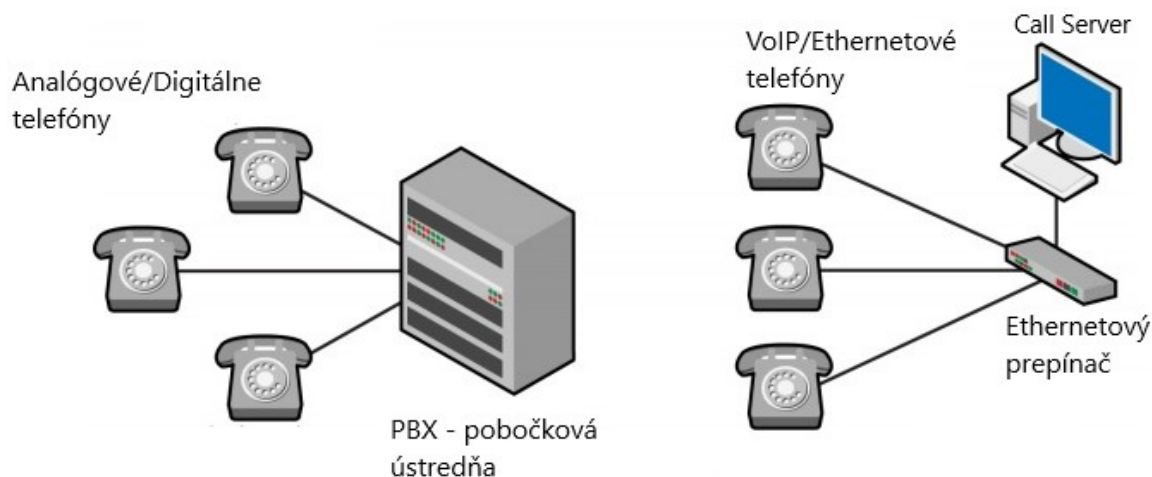
V poslednej časti sa budem venovať zhodnoteniu, využiteľnosti nástroja HOMER 5 v praktickom nasadení, ďalej presnosti prezentovaných dát a taktiež rýchlosti aktualizácie prezentovaných dát.

# 1 Telefónia cez IP protokol

## 1.1 Definícia Voice over the Internet Protocol

Verejná telefónna sieť PSTN - Public Switched Telephone Network, je sieť vybudovaná primárne pre prenos hlasu. PSTN sieť funguje na princípe circuit-switching, teda prepnávanie okruhov. Ide v podstate o pevné prepojenie dvoch komunikačných strán, medzi ktorými prebieha v daný čas telefónny hovor. Akonáhle sa spojí volajúci s volaným, všetka prenosová kapacita tohoto prepojenia je vyhradená len pre daný hovor oboch strán. To zaisťuje veľkú spoľahlivosť a kvalitu prenášaného hlasu.

Voice over IP, teda VoIP funguje na odlišnom princípe. Prenosovým prostredím nie je sieť budovaná pre prenos hlasu, ale internet, teda dátová sieť.[1]. VoIP umožňuje prenos hlasu v sieťach s prepojením paketov založených na protokole IP. VoIP tak tvorí alternatívu ku klasickej telefónii. Táto alternatíva je veľmi perspektívna z dôvodu, že dátové siete sa v súčasnosti rozvíjajú a šíria oveľa rýchlejšie ako telefónne siete, prenos hovorov v dátových sieťach je hlavne ekonomicky výhodný[2].



Obrázok 1.1: Porovnanie tradičného telefónu (vľavo) a VoIP systému (vpravo)

## 1.2 Protokoly využívané vo VoIP

VoIP využíva dva druhy protokolov.

- Signálne - Slúžia k naväzovaniu spojenia, riadeniu toku a jeho ukončovaniu, medzi hlavné protokoly, ktoré sa využívajú patrí SIP a H.323.
- Transportné - Slúžia k vlastnému prenosu hlasu, využívajú sa protokoly RTP a RTCP.

### 1.2.1 Signálne protokoly SIP a H.323

Session Initiation Protocol alebo skrátene SIP je doporučenie od IETF - Internet Engineering Task Force. SIP je signálny protokol per zostavenie, kontrolu a rozpad spojenia medzi dvoma alebo viacerými účastníkmi komunikácie[2]. Medzi najznámejšie spoločnosti, ktoré tento protokol využívajú patrí Skype a Vonage. Práve protokol SIP bude v ďalšej časti bakalárskej práce rozobratý podrobnejšie.

H.323 je súprava štandardov ITU-T. Používa sa napríklad ku riadeniu hovorov a video konferencií. Bol vyvinutý skôr ako ostatné protokoly a to mu zaručilo veľkú používateľnosť naprieč

celým svetom. Používa veľké množstvo signálnych ideí z tradičných telefónov. H.323 využíva rôzne protokoly ako Q.931, H.225, H.245[3].

### 1.2.2 Transportné Protokoly RTP a RTCP

Real-Time Transport Protocol (RTP) je bezpochyby najobľúbenejší protokol pre prenášanie hlasových paketov obsahujúcich hlasové dáta[3]. RTP je definovaný v doporučení RFC 3550[4].

V záhlaví protokolu sú prenášané informácie o type prenášaných dát spôsobe kódovania, zdroja synchronizácie, číslo paketu, časová značka pre obnovenie synchronizácie a real-time vlastností.

Real Time Control Protocol (RTCP) je riadaci protokol spolupracujúci s protokolom RTP, používa periodické vysielanie paketov od každého účastníka RTP relácie všetkým ostatným účastníkom za účelom riadenia výkonu a pre diagnostické účely. Úlohou RTCP sú nasledujúce služby[2]:

- Poskytuje aplikácii informácie týkajúce sa kvality dát.
- Uskutočňuje riadenie intervalu vysielania RTCP.
- Prenos minimálnej informácie o riadení relácie .

## 1.3 SIP - Session Initiation Protocol

V preklade protokol iniciovania relácie, je protokol, ktorého začiatky siahajú do roku 1999 v norme RFC 2543. SIP je textovo založený protokol, ktorý pracuje na aplikačnej vrstve. Protokol SIP je typu klient-server, takže komunikácia prebieha výmenou dvoch typov správ a to žiadostí a odpovedí[5].

### 1.3.1 Komponenty

- **Užívateľský Agent - UA** je logická časť, ktorá iniciuje alebo reaguje na SIP transakcie, čiže sa jedná o koncové body. Užívateľský Agent môže byť klient user Agent Client (**UAC**) alebo server (**UAS**) User Agent Server.
- **Proxy** je medzičlen medzi požiadavkami z UAC do UAS. Toto sa hlavne vykonáva primárne z dôvodu smerovania. Príkladom štandardného nasadenia proxy server. Klient odosiela webové požiadavky na proxy, ktorá ďalej tieto požiadavky posúva na webový server.
- **Server Presmerovania** - Rovnako ako proxa prijíma žiadosti o spojenie od UA alebo proxy serverov, ale neposiela ich ďalej v smere volaného. Posiela tázajúcemu informáciu, komu má žiadosť poslať, abysa dostala k volanému[2].
- **Server Registrácie UAS**, ktorý prijíma registračné správy a aktualizuje polohu[3].

### 1.3.2 Adresovanie

SIP konverzácie môžu začať kontaktovaním konkrétnej IP adresy alebo používateľského mena. Štandardné adresovanie v SIP je veľmi podobné e-mailu. Môže mať niekoľko foriem, číslo portu je 5060[3].

Formy SIP adresovania:

- sip:používateľ@doména:port
- sip:používateľ@host:port
- sip:telefónne číslo@doména

```
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
  > Session Initiation Protocol (INVITE)
    > Request-Line: INVITE sip:150@192.168.23.140 SIP/2.0
    > Message Header
    > Message Body
```

---

Obrázok 1.2: SIP Adresovanie

### 1.3.3 Žiadosti

SIP žiadosti sú využívané k zostaveniu komunikácie.

- **INVITE** - Správa INVITE slúži k iniciovaniu spojenia s užívateľským agentom. Inak povedané správa INVITE slúži k naviazaniu spojenia medzi užívateľmi.
- **BYE** - Správa BYE slúži k ukončeniu spojenia.
- **REGISTER** - Správa REGISTER slúži k registrácii užívateľa. Táto správa je posielaná užívateľom na server.
- **CANCEL** - Správa CANCEL slúži k ukončeniu spojenia, ktoré ešte nebolo naviazané. Užívateľ využíva túto správu v prípade, že chce ukončiť hovor a druhá strana hovor neprijala.
- **OPTIONS** - Správa OPTIONS slúži ako žiadosť o zaslaní prehľadu funkcií podporovaných serverom.
- **ACK** - Správa ACK je používaná ako potvrdenie konečnej odpovedi na správu INVITE. [6].

### 1.3.4 Odpovedi

Na druhej strane sú SIP odpovede, ktoré indikujú, či bola žiadosť úspešná alebo nie. SIP odpoveď je správa generovaná užívateľským agentom UAS.

- **1xx** - Informačná odpoveď, ktorá slúži k indikovaniu prebiehajúceho hovoru. Hlavnou úlohou informačných správ je zamedziť preposielaniu INVITE žiadosti. Typickým zástupcom je správa 180 Ringing alebo 100 Trying.
- **2xx** - Správa indikujúca úspešné akceptovanie žiadosti. Typickým príkladom 200 OK, ktorá prijíma požiadavku o naviazanie spojenia.
- **3xx** - Tieto žiadosti sú posielané serverom presmerovania ako odpoveď na správu INVITE.
- **4xx** - Správa indikujúca chybu na strane klienta užívateľského agenta. Príkladom je správa 400 Bad Request, ktorá indikuje, že server nebol schopný pochopiť požiadavku, napríklad chýbajúce polia pre From, To, Call-ID.
- **5xx** - Táto odpoveď sa používa k indikácii požiadavky, ktorá nemôže byť spracovaná z dôvodu chyby na strane serveru. Príkladom je správa 500 Server Internal Error, ktorá znamená, že na serveri došlo k chybe, ktorá zabraňuje spracovaniu požiadavky.
- **6xx** - Globálna chyba. Indikuje, že požiadavka zlyhá vždy, keď bude otestovaná a to na každom servery.

```

> Frame 9: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits)
> Linux cooked capture
> Internet Protocol Version 4, Src: 192.168.23.155, Dst: 192.168.23.140
> User Datagram Protocol, Src Port: 5060, Dst Port: 5060
▼ Session Initiation Protocol (200)
  > Status-Line: SIP/2.0 200 OK
  ▼ Message Header
    > Via: SIP/2.0/UDP 192.168.23.140:5060;rport;branch=z9hG4bKPjc20d56ce-b94a-4473-b890-ebd167407eb4
    > From: <sip:100@192.168.23.140>;tag=a67bb23c-2996-41d8-8509-12fa30d8eef2
    > To: <sip:192.168.23.155>;tag=818SIPpTag011
    > Call-ID: 963f0003-b312-4c1e-99f9-0653539b67e7
    > CSeq: 26627 INVITE
    > Contact: <sip:192.168.23.155:5060;transport=UDP>
    > Content-Type: application/sdp
    > Content-Length: 139
  > Message Body

```

Obrázok 1.3 SIP odpoveď na žiadosť o registráciu

Obrázok 1.3 Server nám odpoveďou 200OK oznámil, že registrácia prebehla úspešne.

### 1.3.5 Štruktúra SIP hlavičky

Hlavička je komponent SIP správy, ktorá oznamuje informácie o danej správe. Polia SIP hlavičky vo väčšine prípadov nasledujú rovnaké pravidlá ako polia HTTP hlavičky[6]. Nižšie uvedené položky sú tým podstatným výberom z veľkého množstva hlavičiek.

- **TO:** Adresa volaného.
- **FROM:** Adresa volajúceho klienta.
- **VIA:** Adresa klienta, ktorý vysiela požiadavok alebo adresa serverov, cez ktoré daný požiadavok prešiel a kadiaľ sa bude vracat' odpoveď.
- **Call-ID:** Unikátna identifikácia hovoru.
- **Contact:** Aktuálna skutočná adresa klienta.
- **Record-Route:** Zoznam adries servera, ktorý chcú dostávať všetku komunikáciu náležiaciu serveru.
- **Route:** Postupnosť adries serveru, cez ktorý je požiadavok smerovaný.
- **Request-URI (RURI):** Aktuálny adresát požiadavku. Údaj sa vyskytuje v prvom riadku požiadavky za metódou, typom požiadavku[7].

### 1.3.6 SDP - Session description Protocol

Protokol popisu relácie je popísaný v RFC 4566[8]. Zmysel protokolu je v poskytovaní popisu mediálneho obsahu určeného k prenosu, v takom formáte, aby bol pochopiteľný pre účastníkov. Zmyslom protokolu je poskytnutie informácií o mediálnom toku užívateľom, ktorí sa chcú pripojiť do danej relácie alebo za účelom zberu informácií danej relácie[6].

Niektoré parametre SDP:

- **v** = (verzia protokolu)
- **o** = (majiteľ, zakladateľ relácie)
- **s** = (názov relácie)
- **i** =\*(informácie o relácii)
- **e** =\*(emailová adresa)
- **p** =\*(číslo telefónu)
- **c** =\*(informácie o pripojení)

## 2 IP Pobočková ústredňa Asterisk v13

### 2.1 Popis Asterisk

Asterisk je open-source framework pre budovanie komunikačných systémov a aplikácií. Asterisk pracuje na Linuxe a poháňa rôzne pobočkové ústredne, konferenčné servery, VoIP Gatewaye. Projekt je sponzorovaný firmou Digium, ktorá predáva podporu a komerčné produkty.

V roku 1999 prišiel s prvou verziou Asterisku Mark Spencer, ktorý je pre zaujímavosť pôvodným autorom programu dnes známeho pod menom Pidgin.

V Českej republike existujú firmy, ktoré poskytujú komerčný support alebo produkty, ktoré využívajú Asterisk. Sú to napríklad Canistec a IPEX. V práci je zámerne použitá verzia Asterisk 13, čo je Long Term Support, ktorá zaisťuje dlhodobú podporu, ktorá je potrebná pre telefónne ústredne[10].

#### 2.1.1 Podpora protokolu HEP

Veľmi dôležitou funkciou, ktorá bola pridaná už vo verzii 12 je ukladanie SIP signalizácie do externého zdroja. Do Asterisku 12 bola pridaná podpora protokolu HEP - Homer Encapsulation Protocol a dáta ukladá do systému HOMER. Webové rozhranie projektu HOMER následne umožní podrobnú analýzu SIP prevádzky, na starosti majú túto úlohu moduly `res_hep`, `res_hep_pjsip` a `res_hep_rtcp`[10].

### 2.2 Moduly

Asterisk je postavený na moduloch. Modul je načítateľný komponent, ktorý poskytuje špecifickú funkcionality, ako ovládač kanálu, príklad je `chan_sip.so` alebo zdroj, ktorý umožňuje pripojenie k externej technológii, príklad je `func_odbc.so`. Moduly Asterisku sú načítavané zo súboru umiestneného v `/etc/asterisk/modules.conf`. Asterisk je možné spustiť aj bez modulov, ale v tomto štave nebude schopný ničoho[11].

Asterisk obsahuje nasledujúce typy modulov:

- Aplikačné
- Prepojovacie moduly
- Moduly pre zachytávanie detailov hovoru
- Ovládače kanálov
- Prekladače kodekov
- Funkcie pre dialplan
- PBX moduly
- Testovacie moduly
- a ďalšie...

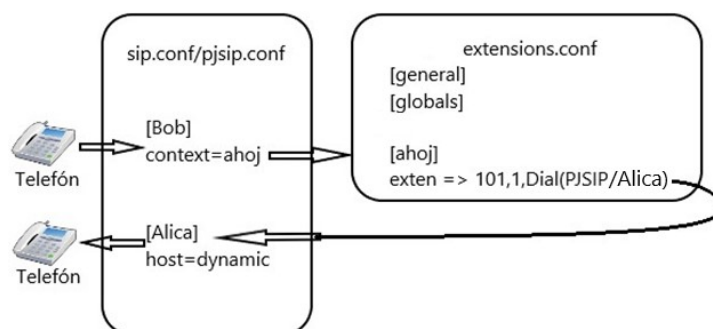
### 2.3 Konfigurácia

Asterisk sa konfiguruje hlavne pomocou textových súborov, ktoré nájdeme v adresári `/etc/asterisk`. Najlepšou cestou ako tieto súbory upraviť je pomocou textového editoru.

- **sip.conf** a **pjsip.conf**: Tieto súbory obsahujú konfiguráciu zariadení, ktoré komunikujú s Asteriskom pomocou SIP protokolu.



- **extensions.conf:** Tento súbor je jadrom ústredne, definuje totiž celý číslovací plán. V tomto súbore definujeme správanie všetkých spojení v ústredni[12].



Obrázok 1.4: Prepojenie medzi sip.conf a extensions.conf

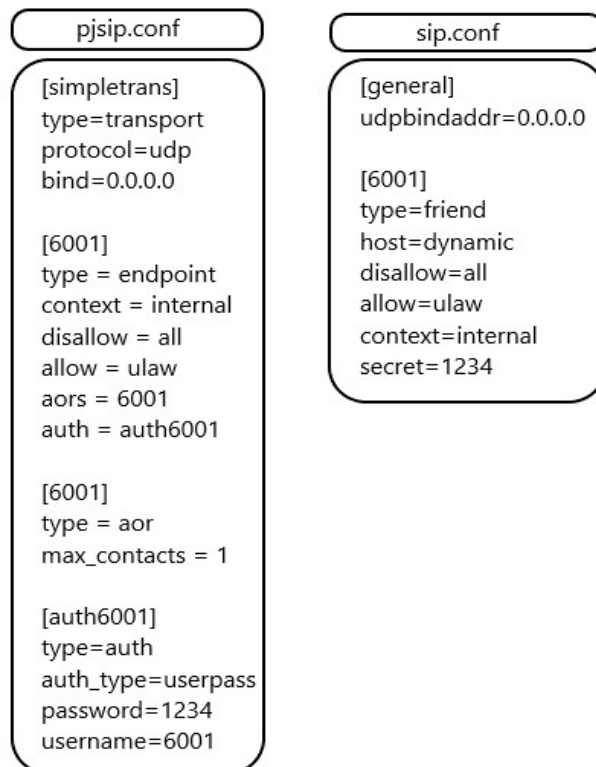
## 2.4 PJSIP

V práci bude namiesto sip.conf využitý pjsip.conf z dôvodu kompatibility s HEP protokolom. PJSIP je voľne dostupná Open Source multimediálna komunikačná knižnica, ktorá implementuje štandardy protokolov ako SIP, SDP, RTP, STUN, TURN a ICE. PJSIP kombinuje signálny protokol SIP s multimediálnou štruktúrou a technológiou NAT do API vysokej úrovne, ktorá je vhodná takmer pre akýkoľvek typ systémov, od stolných počítačov až po mobilné telefóny.

Medzi výhody patrí kompletnosť a integrovanosť, ktorá ponúka vývojárovi všetko, čo potrebuje na zostavenie multimediálnej komunikačnej aplikácie v reálnom čase. Všetky tri hlavné komponenty multimediálnych aplikácií v reálnom čase, tj. signalizácia, mediálne funkcie a prechod NAT sú spravované práve pomocou PJSIP.

Ďalšou výhodou je prenosnosť PJSIP, keď vývojár napíše svoj kód, tak bude spustiteľný na Windows, Mac OS, Linux a ďalších.

Hlavnou výhodou PJSIP je to, že je Open Source Software, čo znamená, že PJSIP je využívaný veľkým množstvom vývojárov po celom svete. Z toho vyplýva, že nájsť PJSIP vývojára je jednoduchšie. Na druhej strane, PJSIP taktiež ponúka licenciu, ktorá je pre tých, ktorí nechcú zverejniť zdroj ich produktov alebo pre tých, ktorí požadujú služby priamo od vývojárov PJSIP[13].



*Obrázok 1.5: Porovnanie sip.conf a pjsip.conf*

Ako môžeme vidieť na Obrázku 1.5, hlavným rozdielom pri nakonfigurovanom jednom koncovom bode je to, že pjsip.conf je rozdelený do sekcií. V práci využívam 4 sekcie, ktoré potrebujem pre funkčnosť a to Transport, Endpoint, AUTH a AOR. Podrobnejšie sa týmto sekciám budem venovať v praktickej časti.

## 3 Monitorovací systém HOMER 5

### 3.1 Popis monitorovacieho systému

HOMER je robustný škálovateľný SIP zachytávací systém a VoIP monitorovacia aplikácia ponúkajúca HEP/EEP zapúzdrenie a zrkadlenie/monitorovanie portov. Je pripravený k uchovávaní veľkého množstva signalizácii, štatistik a záznamov s podporou okamžitého vyhľadávania. Ďalej je pripravený k end-to-end analýze pre providerov VoIP používajúcich SIP signálny protokol.

Jeho používateľské prostredie je jednoducho rozširiteľné a upraviteľné použitím upraviteľných widgetov, ktoré zobrazujú dáta z interných alebo externých zdrojov dát ako InfluxDB a Elasticsearch[14].

Medzi hlavné výhody patrí[15]:

- Okamžitý prístup k predchádzajúcim a budúcim štatistikám signalizácie.
- Jednoduché vyhľadávanie medzi jednotlivými SIP hovormi.
- Automatická korelácia relácii, záznamov, hlásení.
- Podpora pre RTP a RTCP štatistiky a analýzu.
- Vizuálna reprezentácia daného hovoru.
- PCAP export a zdieľanie s inými stranami.
- a mnoho ďalšieho...

### 3.2 Komponenty - Capture Server

Je zodpovedný za zbieranie, indexovanie a ukladanie doručených HEP (HOMER-Encapsulation Protocol) paketov z HEP Agentov. HOMER zachytávací server je založený na SIPCAPTURE Module pre Kamailio a OpenSIPS ponúkajúci optimalizované databázové schémy s pokročilými funkciami. Taktiež obsahuje výkonné a moderné webové používateľské rozhranie[14]. Týmto zachytávacím serverom bude práve môj počítač.

### 3.3 Komponenty - Capture Agents

Sú zodpovední za doručenie HOMERu SIP signalizáciu, RTP/RTCP správy, vlastné štatistiky a mnoho ďalšieho použitím HEP (HOMER-Encapsulation Protocol). Medzi tieto zachytávacie platformy patrí[14]:

- Kamailio
- OpenSIPS
- FreeSWITCH
- Asterisk
- RTP:Engine

### 3.4 HEP - Homer Encapsulation Protocol

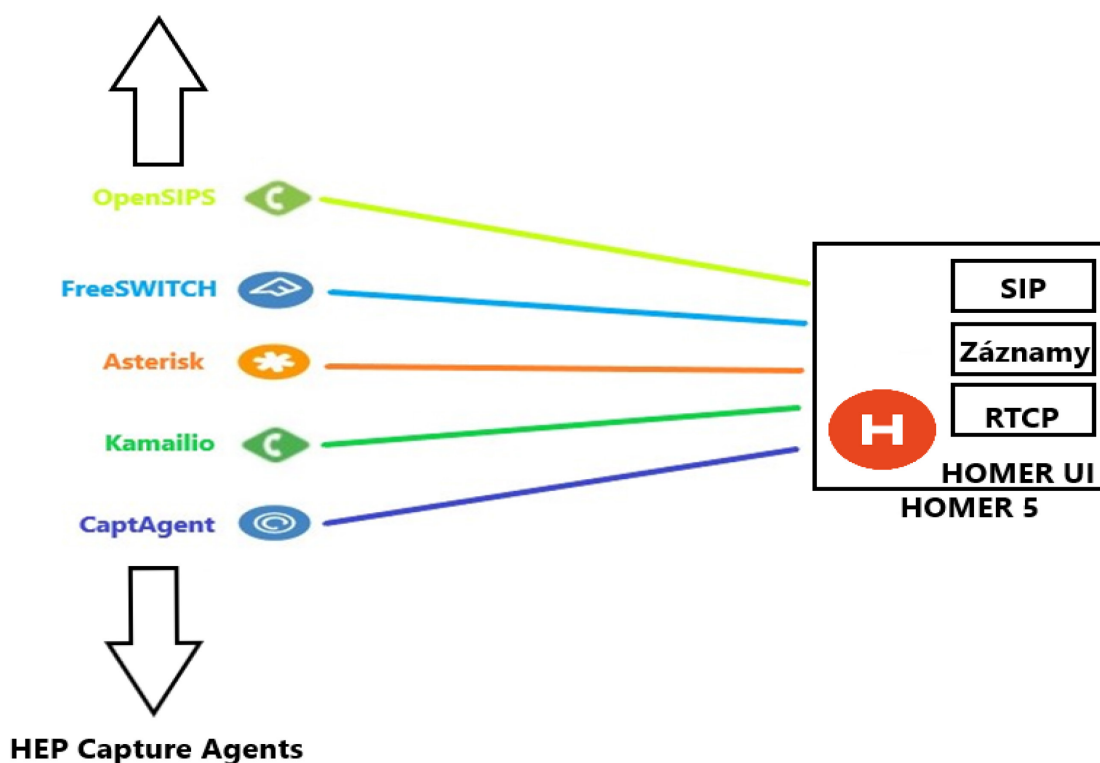
Homer Encapsulation Protocol je používaný k zabaleniu, argumentovaniu a prenosu zachytených paketov medzi zachytávacím agentom a zachytávacím serverom.

HEP protokol bol navrhnutý ako efektívny, modulárny framework, ktorý poskytuje presné duplikovanie pasívne získaných IP datagramov za účelom vzdialeného zbierania cez UDP/TCP/STCP pripojenia. Zachovanie originálneho datagramu a jeho dát musí byť poskytnuté späť zberačom bez zmien alebo straty dát[15].

HOMER momentálne podporuje HEP kódovanie/dekódovanie pre SIP, XMPP, RTCP, RTCP-XR a ďalšie[14].

HEP je tiež podporovaný niekoľkými zachytávacími nástrojmi ako:

- CaptAgent
- Sipgrep
- HEPipe
- nProbe
- sngrep



Obrázok 1.6 Zachytávacie nástroje napojené na HOMER 5

### 3.5 Možnosti inštalácie

HOMER 5 je aplikácia postavená pre operačný systém LINUX, momentálne nie každá linuxová distribúcia je podporovaná[14].

Medzi oficiálne podporované distribúcie patrí Debian 8 a CentOS 7, táto podmienka avšak neplatí v prípade použitia kontajnerovej platformy DOCKER. Dôvod je veľmi jednoduchý, ak daná

distribúcia podporuje DOCKER, tak na nej aj spustíte HOMER 5, tu je distribúcia závislá na podpore DOCKER nie samotného HOMER 5.

HOMER 5 ponúka niekoľko možností pre inštaláciu:

- **Inštalačný skript**, ktorý nainštaluje a nakonfiguruje:  
HOMER 5  
Kamailio 4.4  
MySQL 5.7  
Apache2 a PHP5
- **Pomocou kontajnerovej platformy DOCKER**, ktorý v už predpripravenom obraze spustí v kontajneri:  
HOMER 5  
Kamailio 4.x, na porte 9060  
Apache2 a PHP5 na porte 80  
MySQL5.6/InnoDB na porte 3306
- **Manuálna inštalácia** pre pokročilých používateľov, ktorí si chcú všetko nakonfigurovať podľa seba. Táto možnosť sa odporúča iba pre zdatných používateľov, ktorí majú pokročilé schopnosti v používaní Linuxu[14].

Ja som si v tejto práci zvolil kontajnerovú platformu DOCKER. Podrobnejšie sa "inštalácii" pomocou DOCKERU budem venovať v praktickej časti práce.

### 3.5.1 Kontajnerová platforma DOCKER

DOCKER je platforma pre vývojárov a systémových správcov pre vývoj, distribúciu a beh aplikácií v prostredí linuxových kontajnerov. Koncept Dockeru dovoľuje zostaviť aplikáciu z komponentov a tú potom distribuovať ako celok, bez zmien medzi testovacím a produkčným prostredím. V Dockeri sa často pracuje s pojmami kontajner a obraz (image). V oboch prípadoch sa jedná o nejaké dáta. Obrazom potom rozumieme statický kontajner, ktorý slúži ako predloha pre vytváranie ďalších kontajnerov[16].

## 4 Inštalácia a konfigurácia Asterisk

### 4.1 Inštalácia

Samotná inštalácia prebehla na operačnom systéme Debian 9. Keďže Debian 9 už obsahuje repozitár s Asteriskom a verziou 13, tak samotná inštalácia bola veľmi jednoduchá.

V podstate mi postačili tri kroky. Pomocou terminálu a príkazu **su** som sa prihlásil ako root používateľ, aby som mohol vykonávať zmeny v systéme.

Ďalší krok bolo použitie príkazu pre aktualizáciu inštalačných balíčkov:

- **apt-get update**

Potom som už mohol zadať príkaz pre inštaláciu samotného Asterisku:

- **apt-get install asterisk**

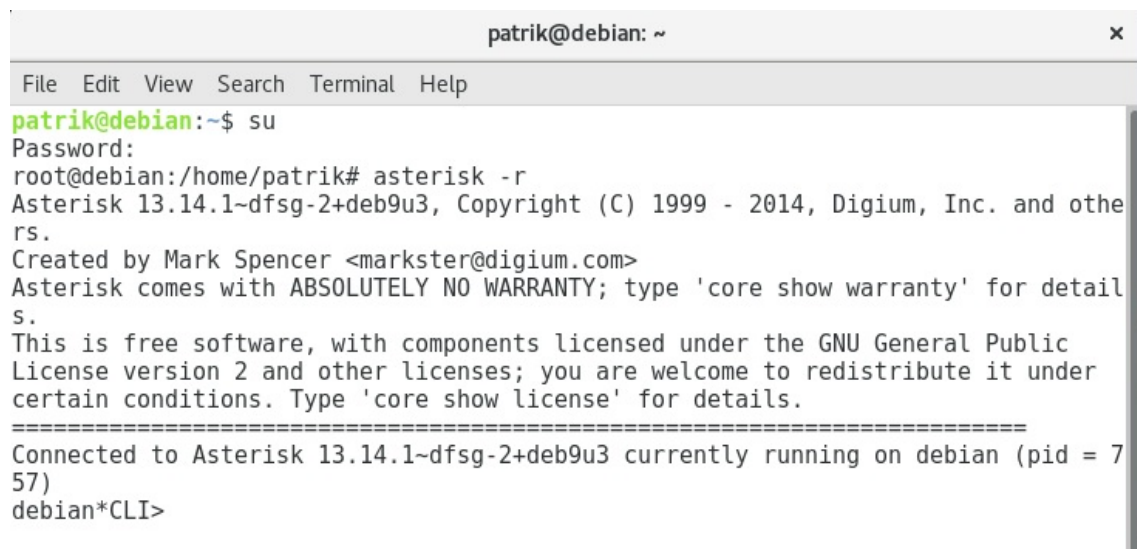
Týmto príkazom sa spustí inštalácia, po úspešnom nainštalovaní je Asterisk pripravený k používaniu.

Do konzoly Asterisku sa prihlásime pomocou príkazu, ktorý zadáme do terminálu:

**asterisk -r**

alebo

**asterisk -vvvvvv**

A screenshot of a terminal window titled 'patrik@debian: ~'. The terminal shows the user 'patrik@debian' at the prompt '~\$' typing 'su'. After a password prompt, the user is at the root prompt 'root@debian:/home/patrik#'. They type 'asterisk -r'. The terminal displays the Asterisk version '13.14.1~dfsg-2+deb9u3', copyright information, and a license notice. It then shows 'Connected to Asterisk 13.14.1~dfsg-2+deb9u3 currently running on debian (pid = 757)' and the prompt 'debian\*CLI>'.

```
patrik@debian: ~  
File Edit View Search Terminal Help  
patrik@debian:~$ su  
Password:  
root@debian:/home/patrik# asterisk -r  
Asterisk 13.14.1~dfsg-2+deb9u3, Copyright (C) 1999 - 2014, Digium, Inc. and others.  
Created by Mark Spencer <markster@digium.com>  
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.  
This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.  
=====
```

Obrázok 1.7: Príkazový riadok Asterisku

## 4.2 Konfigurácia

Konfigurácia Asterisku je celkom priamočiara, ale konfigurácia samotného serveru nestačí, tiež je potrebné nakonfigurovať samotné zariadenie, aby vedelo kam posielat' hovor.

Takže je potrebné urobiť dve úlohy, aby bolo zariadenie schopné spolupracovať a Asteriskom.

- Povedať Asterisku o zariadení.
- Povedať zariadení o Asterisku.

**sip.conf** je kanálový modul, ktorý má najviac funkcií z pomedzi všetkých modulov v Asterisku. Toto je spôsobené aj obrovskou popularitou SIP protokolu.

Ako som už spomenul v odseku 2.4, mňa bude v tejto práci zaujímať konfiguračný súbor **pjsip.conf**, ktorý je využitý z dôvodu kompatibility s HEP protokolom a číslovací plán **extensions.conf**.

Súbor **pjsip.conf** sa nachádza v **/etc/asterisk**

Súbor **pjsip.conf** tvoria sekcie, každá sekcia definuje konfiguráciu pre konfiguračný objekt. Sekcie sú identifikované menami v hranatých zátvorkách.

Ako som už spomenul v odseku 2.4 v práci využívam 4 sekcie, ktoré mi zaručujú funkčnosť a to Transport, Endpoint, AUTH a AOR.

- **Endpoint alebo Koncový bod**

Konfigurácia koncového bodu poskytuje rozne možnosti, ktoré súvisia s jadrom funkcionality SIP a viaže sa na ostatné sekcie ako AUTH, AOR a Transport. Bez pridelenia AoR sekcie nemožem kontaktovať koncový bod. Je to profil pre koncový bod ako napríklad telefón alebo vzdialený server.

- **Transport**

Nakonfiguruje ako bude **pjsip** pracovať. Oproti **sip.conf** poskytuje viac možností. Podporuje konfiguráciu pre protokoly ako TCP, UDP alebo WebSocket a šifrovacie metódy ako TLS/SSL.

- **AUTH**

Autentizačné sekcie držia možnosti a údaje spojené s prichádzajúcou alebo odchádzajúcou autentizáciou.

- **AOR**

Hlavnou úlohou AoR - Address of Record je povedať Asterisku kde môžu byť koncové body kontaktované. Bez pridelenej AOR sekcie nemôže byť koncový bod kontaktovaný[18].

Všetky tieto časti riadi modul **res\_pjsip** a jeho načítanie uskutočníme zadáním príkazu **module load res\_pjsip.so** do konzoly Asterisku.

Takže som rozobral časti potrebné pre konfiguráciu **pjsip.conf**, teraz môžem upraviť svoj vlastný súbor. Ako som už spomenul, súbor je umiestnený v **/etc/asterisk**. Pre prístup a úpravy tohoto

súboru som použil nástroj midnight commander, ktorý mi umožní prehľadné orientovanie sa v adresároch, na samotné úpravy som použil textový editor nano, root práva sú samozrejmosťou. Súbor pjsip.conf som si upravil nasledovne:

```
[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0

[ bob ]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=bob
aors=bob

[ bob ]
type=auth
auth_type=userpass
password=bob
username=bob

[ bob ]
type=aor
max_contacts=10
```

Nakonfiguroval som si dva koncové body jeden je **Bob**, moju konfiguráciu môžeme vidieť vyššie a rovnako ako Boba som si nakonfiguroval aj druhý koncový bod **Alica**. Pre prenos je využitý protokol UDP.

Po úspešnom upravení pjsip.conf si ešte musím upraviť súbor **extensions.conf**. Súbor extensions.conf obsahuje číslovací plán Asterisku. Kontroluje prichádzajúce hovory a ich smerovanie. Toto je súbor kde nastavím správanie všetkých pripojení cez moju PBX. Tento súbor sa rovnako ako pjsip.conf nachádza v **/etc/asterisk**

Ja som si extensions.conf upravil nasledovne:

```
[internal]

exten=> bob,1,Dial(PJSIP/bob,20)
exten=> alica,1,Dial(PJSIP/alica,20)
```



V hranatej zátvorke názov `internal` značí len kontext, môže byť kľudne nazvaný podľa vlastného uváženia, hlavné je aby sa tieto názvy kontextu zhodovali so súborom `pjsip.conf`, ja som zvolil názov `internal`. Ďalej sa pod kontextom nachádza `exten=> bob,1,Dial(PJSIP/bob,20)`, ktoré skúša kontaktovať Boba po dobu 20 sekúnd, to isté platí pre Alicu. Po pridaní a uložení súboru je nutné zadať do príkazového riadku Asterisku príkaz **dialplan reload** a to z dôvodu načítania týchto údajov. Pomocou príkazu `dialplan show internal` môžeme overiť, či sa informácie načítali správne.

Po nakonfigurovaní a uložení som zadal už spomenutý príkaz **dialplan reload** pre načítanie súboru a overil som pomocou výpisu cez príkaz **dialplan show internal** pridané koncové body.

```
'Alica' =>          1. Dial(PJSIP/Alica,20)          [pbx_config]
'Bob'  =>          1. Dial(PJSIP/Bob,20)          [pbx_config]
```

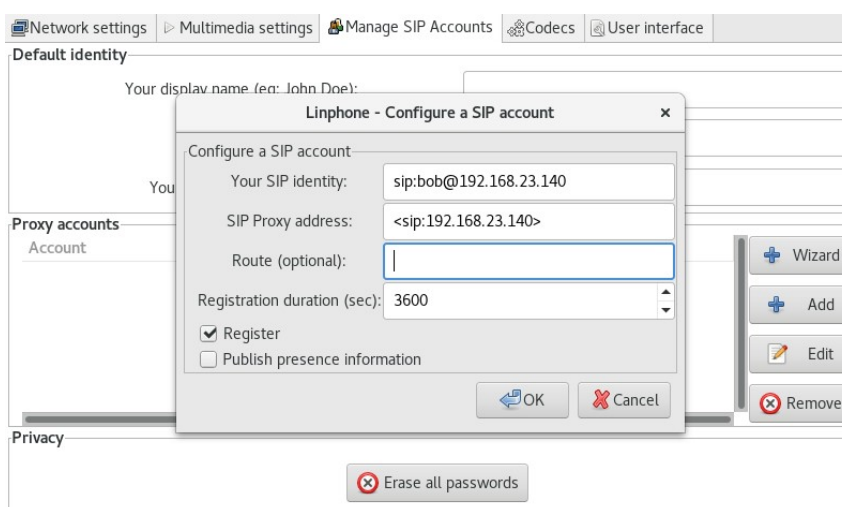
Obrázok 1.8: Overenie správnosti načítania `extensions.conf`

Po úspešnom nastavení a nakonfigurovaní Asterisku, môžem pokračovať v navrhovaní testovacieho prostredia. To pre mňa znamená, že som splnil prvý bod a to nakonfigurovanie serveru, čo znamená presne to, čo som už spomenul na začiatku tohoto odseku, teda povedať Asterisku o zariadení.

Teraz ma čaká splnenie druhého bodu a to povedať zariadení o Asterisku, o chvíľu rozoberiem ako som postupoval.

### 4.3 Registrácia koncových bodov pomocou LinPhone

Teraz ma čaká zaregistrovanie účastníkov na mnou vytvorený Asterisk server. Na tento účel som si vybral VoIP telefón LinPhone, ktorý využíva SIP protokol a umožňuje slobodnú komunikáciu s účastníkmi cez internet pomocou hlasových, textových správ alebo videa[21]. Inštalácia je veľmi jednoduchá, uskutočnil som ju pomocou príkazu **apt-get install linphone**. Inštaláciu som vykonal na dvoch virtuálnych počítačoch s linuxovou distribúciou Debian. Po spustení LinPhone si zaregistrujem účastníka na Asterisk, cesta pre registráciu v LinPhone je **Options -> Preferences -> Manage SIP Accounts**, pomocou tlačidla **Add** si zaregistrujem účastníka.



Obrázok 1.9: Registrácia účastníka pomocou LinPhone

Ako vidíte na obrázku 1.9, pre registráciu som si vybral užívateľa Bob, ktorého SIP adresa alebo aj identita je **sip:bob@192.168.23.140**, kde IP 192.168.23.140 je adresa môjho Asterisk serveru. Po zadaní adresy, ktorá je sip:192.168.23.140 a stlačení OK bude ešte používateľ vyzvaný o zadanie hesla, ktoré bolo v mojom prípade rovnaké ako meno užívateľa a to bob, viz.

Rovnaký proces registrácie som zopakoval aj na druhom virtuálnom počítači s užívateľom Alica. Registrácia prebehla úspešne, tak môžem vykonať testovací hovor.

Po úspešnom otestovaní môžem usúdiť, že moja Asterisk PBX je nakonfigurovaná správne.

## 5 Spojazdenie systému HOMER 5

### 5.1 DOCKER - Inštalácia

Ako prvú vec si musíme nainštalovať samotný DOCKER. Inštalácia je na distribúciach Debian/Ubuntu veľmi jednoduchá.

Do terminálu sa prihlásime ako root používateľ. Začneme dobre známym príkazom pre aktualizáciu balíčkov:

- **apt-get update**

Ďalším podstatným príkazom je:

- **apt-get install apt-transport-https ca-certificates curl software-properties-common**

Tento príkaz povolí **apt** používanie repozitára cez HTTPS.

Príkaz:

- **curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -**

Príkaz na pridanie oficiálneho DOCKER GPG kľúča.

Teraz môžeme zadať príkaz na inštaláciu samotného Dockeru:

- **apt-get install docker-ce**

Príkaz, ktorý spustí inštaláciu DOCKER.

Po dokončení by mal byť DOCKER úspešne nainštalovaný. Funkčnosť DOCKERU si môžeme overiť pomocou príkazu:

- **docker run hello-world**

Tento príkaz stiahne testovací obraz a spustí ho v kontajneri. Akonáhle sa kontajner spustí, ukáže nám informačnú správu[22].

```
root@ubuntu:/home/test# docker run hello-world

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://cloud.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/engine/userguide/
```

Obrázok 2.0: Úspešná inštalácia Docker

## 5.2 Spustenie systému HOMER 5 pomocou platformy DOCKER

Po úspešnom nainštalovaní nasleduje spustenie samotného monitorovacieho systému HOMER 5 pomocou platformy Docker.

Pri Dockeri nemôžeme hovoriť o inštalácii, pretože nič neinštaluje, len stiahne predpripravený obraz, ktorý spustí a na základe stiahnutého obrazu vytvorí kontajner. HOMER 5 ponúka dve možnosti a to spustenie v multi-kontajnerovom režime alebo spustenie v jednom kontajneri.

Nakoľko ja nepotrebujem rozdeliť HOMER do viacerých kontajnerov, postačí mi riešenie s jedným kontajnerom, ktoré ponúka všetko potrebné.

Celý HOMER 5 bude fungovať ako localhost, vrátane databázy.

Príkaz:

- **docker run -it -v /tmp/homer\_mysql:/var/lib/mysql --name homer5 -p 80:80 -p 9060:9060/udp sipcapture/homer-docker**

stiahne a spustí predpripravený obraz a na základe tohto obrazu spustí kontajner.

Ja som si príkaz troška upravil podľa svojich potrieb.

- **docker run -d -v homer\_mysql:/var/lib/mysql --name homer -p 80:80 -p 9060:9060/udp sipcapture/homer-docker**

V príkaze nastala zmena z -it na -d, -d znamená detached. Kontajner je spustený na pozadí.

Druhou zmenou je malé upravenie cesty kam sa budú ukladať dáta, keby túto cestu nemám špecifikovanú, tak by sa po každom reštarte uložené dáta zmazali.

Treťou a poslednou zmenou je zmena pomenovania kontajneru z homer5 na homer.

Po stiahnutí s úspešnom spustení kontajneru je HOMER 5 plne funkčný a pripravený na použitie.

Príkazom **docker ps** si môžeme vypísať aktuálne spustené kontajnery. Popríklad **docker ps -a** nám vypíše všetky kontajnery, aj tie ktoré sú momentálne pozastavené.

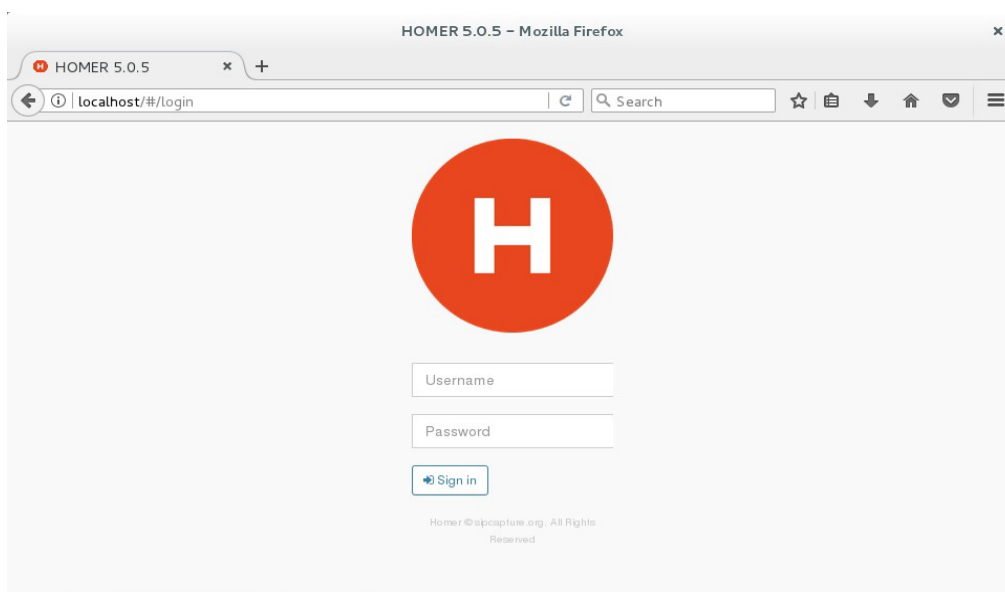
Po každom reštarte počítača je kontajner potrebné znova spustiť. Spustenie uskutočníme príkazom:

- **docker start homer**

Týmto si kontajner spustíme a HOMER je pripravený na použitie. Príkazom **docker stop homer** zasa kontajner v prípade potreby zastavíme.

### 5.3 Užívateľské rozhranie

Do užívateľského rozhrania sa prihlásime cez internetový prehliadač pomocou IP adresy **192.168.23.157**, toto je zároveň aj ip môjho počítača. Druhou možnosťou je namiesto IP napísať do prehliadča jednoducho localhost.

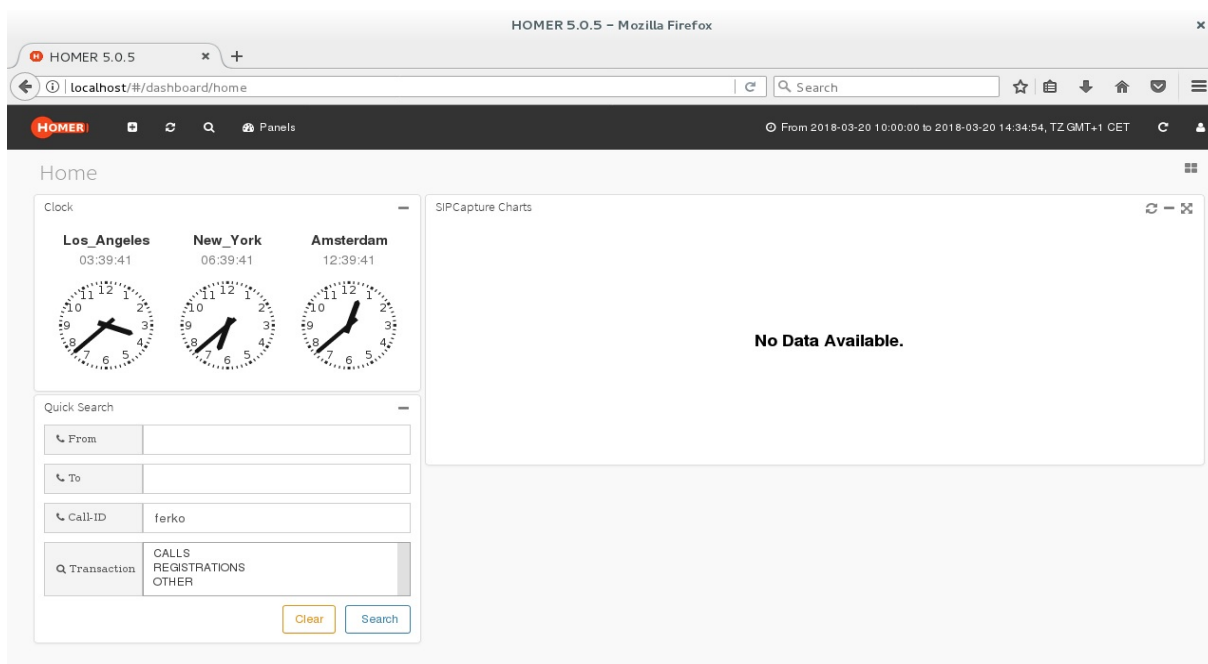


*Obrázok 2.1: Prihlasovacia obrazovka HOMER 5*

HOMER 5 má predovšetkým prihlasovacie údaje:

- **Username: admin**
- **Password: test123**

Tieto údaje si samozrejme môže užívateľ zmeniť podľa svojich potrieb. Po zadaní prihlasovacích údajov sa konečne dostaneme do užívateľského prostredia HOMER 5.



Obrázok 2.2: Užívateľské rozhranie HOMER 5

V prípade úspešného prihlásenia sa dostaneme do užívateľského rozhrania, ktoré môžeme vidieť na Obrázku 2.2. Ako môžeme vidieť na prednastavenej obrazovke sa nachádzajú rôzne okná, môžeme vidieť napríklad svetový čas, rýchle vyhľadávanie a SIPCapture Charts, teda grafy.

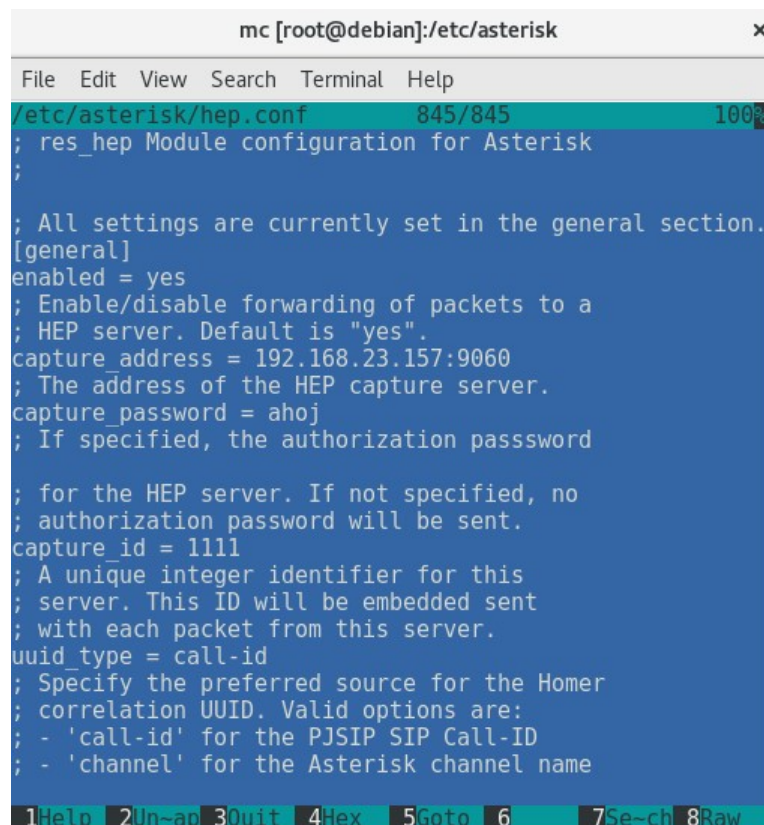
Pre mňa je podstatné okno práve rýchle vyhľadávanie a SIPCapture Charts, v ktorom sa budú zobrazovať moje dáta. Samozrejme HOMER 5 obsahuje ďalšie zaujímavé funkcie, medzi ktorými sa môžeme prepínať pomocou tlačidla "Panels" v ľavom hornom rohu. Niektoré funkcie postupne rozoberem neskôr v práci.

Keďže v okne SIPCapture Charts sa nenachádzajú dáta, tak mojou ďalšou úlohou je tento stav zmeniť a pomocou HEP protokolu prepojiť Asterisk s HOMER 5.

## 5.4 Prepojenie HOMER 5 a Asterisk pomocou HEP protokolu

HEP (res\_hep) je schopný natívne zrkadliť pakety do zberača, ktorým je HOMER. Samotná konfigurácia a prepojenie v prípade použitia PJSIP a SIPp je veľmi jednoduchá.

V adresári Asterisku, ktorého cesta je `/etc/asterisk` sa nachádza konfiguračný súbor **hep.conf**. Tento súbor si musím upraviť tak, aby Asterisk odosielať pakety HOMERU.



```
mc [root@debian]:/etc/asterisk
File Edit View Search Terminal Help
/etc/asterisk/hep.conf 845/845 100%
; res_hep Module configuration for Asterisk
;
; All settings are currently set in the general section.
[general]
enabled = yes
; Enable/disable forwarding of packets to a
; HEP server. Default is "yes".
capture_address = 192.168.23.157:9060
; The address of the HEP capture server.
capture_password = ahoj
; If specified, the authorization password
; for the HEP server. If not specified, no
; authorization password will be sent.
capture_id = 1111
; A unique integer identifier for this
; server. This ID will be embedded sent
; with each packet from this server.
uuid_type = call-id
; Specify the preferred source for the Homer
; correlation UUID. Valid options are:
; - 'call-id' for the PJSIP SIP Call-ID
; - 'channel' for the Asterisk channel name
1Help 2Un~ap 3Quit 4Hex 5Goto 6 7Se~ch 8Raw
```

Obrázok 2.3: Nakonfigurovaný súbor *hep.conf*

Ako môžeme vidieť na Obrázku 2.3, nakonfiguroval som si konfiguračný súbor *hep.conf*. Všetky nastavenia sa nachádzajú v sekcii `[general]`.

- **enabled = yes**, je podmienka pre funkčnosť, štandardne je táto funkcia už povolená.
- **capture\_address = 192.168.23.157:9060**, špecifikovanie HEP zachytávacieho serveru, teda HOMER.
- **capture\_password = ahoj**, nie je podmienkou, môže a nemusí byť špecifikované.
- **capture\_id = 1111**, celé číslo, ktoré slúži ako unikátny identifikátor serveru a je posielaný s každým paketom.
- **uuid\_type = call\_id**, špecifikovanie preferovaného zdroja pre HOMER, "call\_id" pre PJSIP SIP Call-ID, druhá možnosť "channel" pre názov kanálu Asterisku.

Týmto mám *hep.conf* nakonfigurovaný, ale mimo konfigurácie je ešte vyžadované načítanie modulu *res\_hep\_pjsip.so* potrebného pre funkčnosť.

Tento modul načítam tak, že do konzoly Asterisku som si zadal príkaz **module reload res\_hep\_pjsip.so**. Po vykonaní tohoto kroku je konfigurácia dokončená a Asterisk bude preposielať dáta na HOMER.

Funkčnosť si overím jednoducho tým, že uskutočním hovor a počkám, či sa mi nejaké dáta objavia v prostredí HOMERu alebo si na strane HOMERu počas toho ako prebieha hovor pomocou aplikácie *tcpdump* odchytiť na konkrétnom rozhraní prenos a uvidím, či Asterisk nejaké dáta na môj HOMER server odosiela.



Ako prvé som si pomocou aplikácie tcpdump, ktorá slúži ako analyzátor paketov overil, či mi Asterisk posielal HEP pakety na môj HOMER server. Tcpdump sa nainštaluje jednoducho pomocou príkazu **apt-install tcpdump**. Na virtuálny počítač s HOMER som pomocou príkazu **tcpdump -nqt -s 0 -A -i ens33 port 9060** spustil zachytávanie správ na rozhraní ens33 a porte 9060, čo je port ktorý využíva HEP protokol.

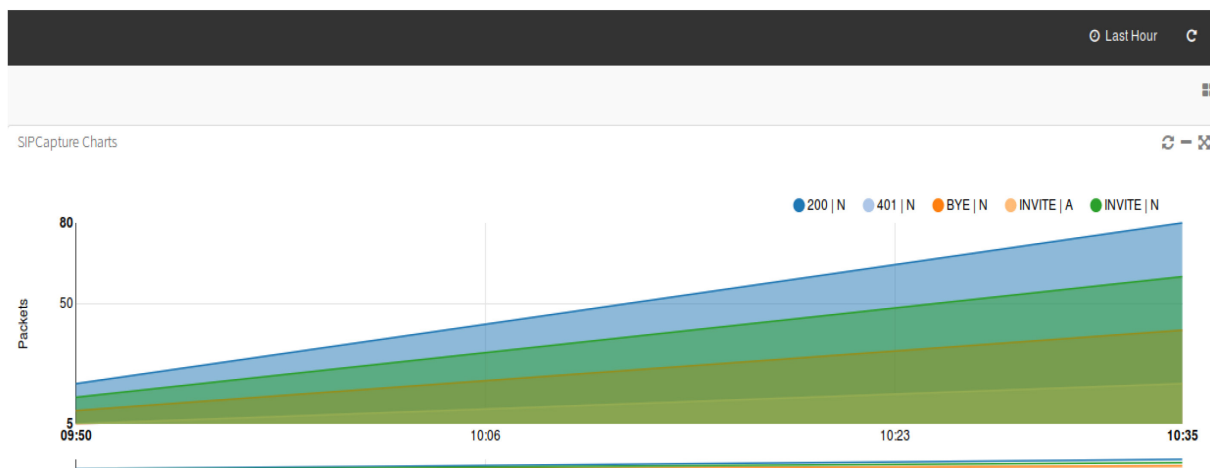
```
root@ubuntu:/home/test# tcpdump -nqt -s 0 -A -i ens33 port 9060
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
IP 192.168.23.140.42635 > 192.168.23.157.9060: UDP, length 664
E...`.@.'.....#d....HEP3.....
Z..h...
.
..a.....
...W.....
.....
.....
ahoj.....1-784@192.168.23.156.....INVITE sip:150@192.168.23.140 SIP/2.0
Via: SIP/2.0/UDP 192.168.23.156:5060;branch=z9hG4bK-784-1-1
From: <sip:100@192.168.23.140>;tag=784SIPpTag001
To: <sip:150@192.168.23.140>
Call-ID: 1-784@192.168.23.156
CSeq: 1 INVITE
Contact: <sip:100@192.168.23.156:5060>
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 161

v=0
o=100 53655765 2353687637 IN IP4 192.168.23.156
s=-
c=IN IP4 192.168.23.156
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 PCMA/8000
a=ptime:20
a=sendrecv
```

Obrázok 2.4: Úspešné odcyhtenie HEP paketu pomocou tcpdump

Výsledok môžeme vidieť na Obrázku 2.4, po začatí hovoru začala prichádzať z Asterisku komunikácia, vybral som si správu INVITE, na ktorej je podrobne vypísaná celá správa. Týmto môžem usúdiť, že nakonfigurovanie HEP protokolu prebehlo úspešne a teraz si môžem skúsiť, či sa mi dáta budú zobrazovať aj priamo v prostredí HOMERu.





Obrázok 2.5: Dáta zobrazené v HOMER

Ako môžeme vidieť na Obrázku 2.5, po uskutočnení hovoru sa mi konečne zobrazili dáta ohľadne mojej SIP komunikácie. Môžeme prehľadne vidieť farebne zobrazené jednotlivé SIP správy, podrobnejšiemu rozboru sa budem venovať neskôr. Dôležitým faktorom je správne nastavenie časového úseku, ktorý chceme analyzovať, inak sa nám dáta nezobrazia. Ja som v pravom hornom rohu vyznačil môj úsek, ktorý chcem analyzovať, čiže poslednú hodinu minút.

Ak sa dáta nezobrazujú aj v prípade správneho nastavenia časového úseku, tak odporúčam skontrolovať, či máte správne zosynchronizované časové pásma na HOMER, aj na Asterisk servery. V prípade, že nie môže sa stať, že dáta sa síce v HOMER nachádzajú, ale nezobrazia sa z dôvodu, že prišli v iný čas ako máte nastavený časový úsek, čo môže vyústiť v nepríjemné a hlavne zbytočné problémy.

Takže prepojenie medzi Asterisk a HOMER mám úspešne za sebou a môžem sa posunúť ďalej.

## 6 Testovací nástroj SIPp

SIPp je nástroj na testovanie výkonu pre SIP protokol. Obsahuje niekoľko základných UAS a UAC scenárov vo formáte .xml.

Taktiež umožňuje čítanie XML scenárov popisujúcich hocikáku testovaciu konfiguráciu. Ponúka dynamické zobrazenie štatistík o práve prebiehajúcom teste. SIPp môže byť použitý v mnoho SIP zariadeniach ako SIP proxy, B2BUA, SIP media servery a SIP PBX. Taktiež je veľmi užitočný na simulovanie a napodobňovanie tisícok SIP systémov[17].

### 6.1 Inštalácia

Inštalácia je mierne zložitejšia, nakoľko je potrebné pred samotnou inštaláciou SIPp nainštalovať aj niektoré knižnice a C++ kompilátor.

Po prihlásení ako root používateľ zadáme už známy príkaz na aktualizáciu balíčkov

- **apt-get update.**

Ďalším krokom je nainštalovanie C++ kompilátora pomocou príkazu:

- **apt-get install build-essential**

Ďalej nasleduje inštalácia OpenSSL:

- **apt-get install openssl libssl1.0-dev**

Inštalácia knižníc ncurses a curses:

- **apt-get install libncurses5-dev libncursesw5-dev**

Inštalácia libpcap a libnet:

- **apt-get install libpcap-dev libnet-pcap-perl**

Teraz nasleduje stiahnutie .tar.gz balíčka, ale najprv si vytvoríme priečinok kam chceme súbor uložiť, príkaz `mkdir sipp` (make directory) vytvorí priečinok sipp a pomocou príkazu `cd sipp` (change directory) sa do tohoto priečinku premiestnime.

Pomocou príkazu `wget` (webget) a odkazu na súbor sipp:

- **wget https://github.com/SIPp/sipp/releases/download/v3.5.1/sipp-3.5.1.tar.gz**

Stiahneme aktuálnu verziu 3.5.1, ktorú ešte musíme nainštalovať.

Príkaz **tar -xvzf sipp-3.5.1.tar.gz** rozbalí inštalačný balíček do sipp adresára.

Teraz sa musíme do rozbaleného adresára premiestniť, umožní to príkaz **cd sipp-3.5.1**, po rozbalení použitím príkazu **./configure --with-openssl --with-pcap**, tento príkaz je zodpovedný za prípravu a nakonfigurovanie, vlastne zistí či je všetko potrebné pripravené pre inštaláciu.

Ako posledný je príkaz **make**, ktorý zostaví a pripraví samotný SIPp. SIPp mám teraz pripravený na použitie.

## 6.2 Konfigurácia

Po úspešnej inštalácii sa môžem pustiť do realizácie funkčnosti. SIPp sa ovláda v príkazovom riadku, čiže jeho užívateľské rozhranie je príkazový riadok.

Rovnako ako pri LinPhone budem využívať dva virtuálne počítače jeden UAC a druhý UAS, komunikáciu bude riadiť znova mnou nakonfigurovaný Asterisk server.

Tak ako aj pri konfigurácii LinPhone Bob a Alica, aj tu si musím najprv upraviť súbory **pjsip.conf** a **extensions.conf** a charakterizovať koncové body a číslovací plán. Vytvoril som si 100 koncových bodov. Tieto koncové body si budú vymieňať signalizáciu medzi sebou, ktorú budem neskôr analyzovať.

```
[transport-udp]
type=transport
protocol=udp
bind=0.0.0.0

[endpoint] (!)
type=endpoint
context=internal
disallow=all
allow=alaw
direct_media=no

[149] (endpoint)
auth=149
aors=149

[149] (auth)
[149] (aor-uac)

[aor-uas] (!)
type=aor
contact=sip:192.168.23.155

[aor-uac] (!)
type=aor
contact=sip:192.168.23.156

[150] (endpoint)
auth=150
aors=150

[150] (auth)
[150] (aor-uas)
```

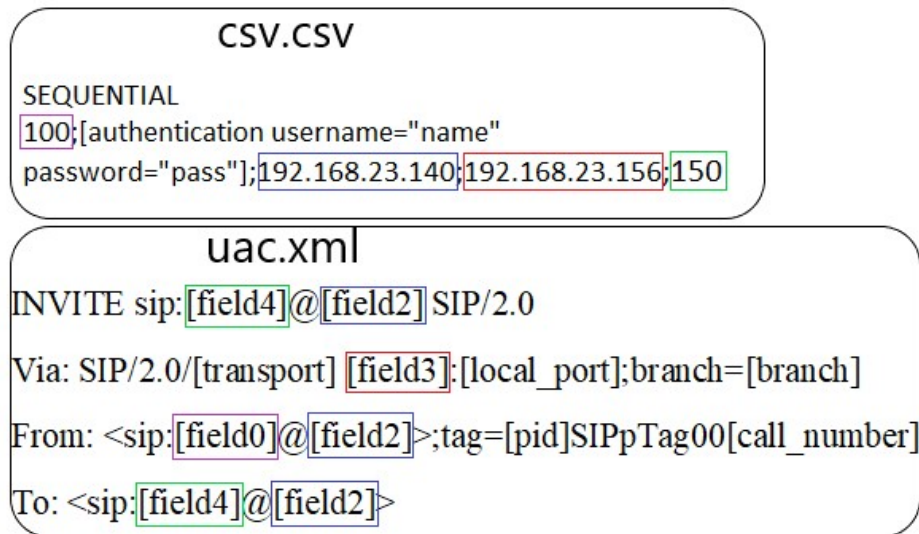
Vyššie môžeme vidieť príklad môjho pjsip.conf súboru, ktorý bude využitý nástrojom SIPp. Má, nadefinovanú šablónu so sekciami podľa ktorej som si vygeneroval koncové body, ktoré z tejto šablóny dedia. Koncové body 100 až 149 predstavujú UAC, teda klient a koncové body 150 až 199 predstavujú UAS, teda server. Medzi týmito koncovými bodmi budú uskutočňované hovory.

Ďalej si musím upraviť súbor extensions.conf, môj som upravil nasledovne:

```
exten => _1XX,1,Dial(PJSIP/${EXTEN},20)
```

Nesmiem zabudnúť na načítanie týchto súborov. Toto uskutočním už známymi príkazmi do konzoly Asterisku **module load res\_pjsip.so** a **dialplan reload**.

Po upravení a úspešnom načítaní si musím ešte vytvoriť a vygenerovať súbor .csv, ktorý obsahuje dáta o užívateľoch, tieto dáta bude využívať UAC scenár.



Obrázok 2.6: Prepojenie medzi .xml scenárom a .csv súborom

Na Obrázku 2.6 môžeme vidieť ako si scenár dopĺňa dáta z .csv súboru.

Pole 0: koncový bod 100

Pole 2: IP adresa Asterisk serveru

Pole 3: IP adresa UAC

Pole 4: koncový bod 150

Po týchto krokoch si môžeme otestovať funkčnosť

Na strane UAS zadám a spustím príkaz:

**sipp -sf uas.xml -m 10 -i 192.168.23.155**

- Ako scenár **uas.xml** som použil ten, ktorý je už priamo predpripravený v SIPp a ktorý na moje testy plne postačuje. Tento základný scenár som si vygeneroval príkazom **sipp -sd uas > uas.xml**.
- **-m 10** znamená počet hovorov.
- **192.168.23.155** je adresa môjho UAS serveru.

Po spustení príkazu UAS si musím následne spustiť príkaz na strane UAC.

Príkaz je nasledovný:

**sipp -sf uac.xml -inf csv.csv -set call\_duration 10000 -r 1 -rp 1s -m 10 -i 192.168.23.156 -p 5060 -l 10000 192.168.23.140**

- Scenár **-sf uac.xml** som mal predpripravený vedúcim práce, tak aby bol schopný komunikovať so súborom .csv.
- **-inf csv.csv** špecifikuje názov súboru, odkiaľ si bude UAC scenár dopĺňať údaje o koncových bodoch.

- - **set call\_duration 10000** je dĺžka hovoru v mili sekundách, čiže momentálne mám nastavené aby jeden hovor trval 10 sekúnd.
- -**r 1** špecifikovanie koľko hovorov sa vykoná za -rp, -**rp 1s** špecifikovanie frekvencie pre -r, čiže ja mám pomer 1 hovor/sekunda, napríklad keby mám -r 6 a -rp 2s, tak mám 3 hovory/sekunda.
- **192.168.23.156** IP adresa UAC klienta.
- -**p 5060** zadefinovanie portu ktorý využíva SIP.
- **192.168.23.140** IP adresa Asterisk serveru[23].

Či je všetko nakonfigurované správne zistím jednoducho a to tak, že medzi UAC a UAS začne prebiehať komunikácia.

Po dokončení sa na strane UAC aj UAC vypíše tabuľka, či boli hovory úspešné alebo naopak, či nastali nejaké chyby. V prípade úspešnej komunikácie sa na strane UAC vypíše tabuľka s:

Tabuľka 1.1: *Výpis UAC po dokončení komunikácie*

|                       |                 |
|-----------------------|-----------------|
| Incoming call created | 0               |
| Outgoing call created | 10              |
| Total Call created    | 10              |
| Successful call       | 10              |
| Failed call           | 0               |
| Call Length           | 00:00:10:016000 |

A na strane UAS sa zasa vypíše tabuľka s:

Tabuľka 1.2: *Výpis UAS po dokončení komunikácie*

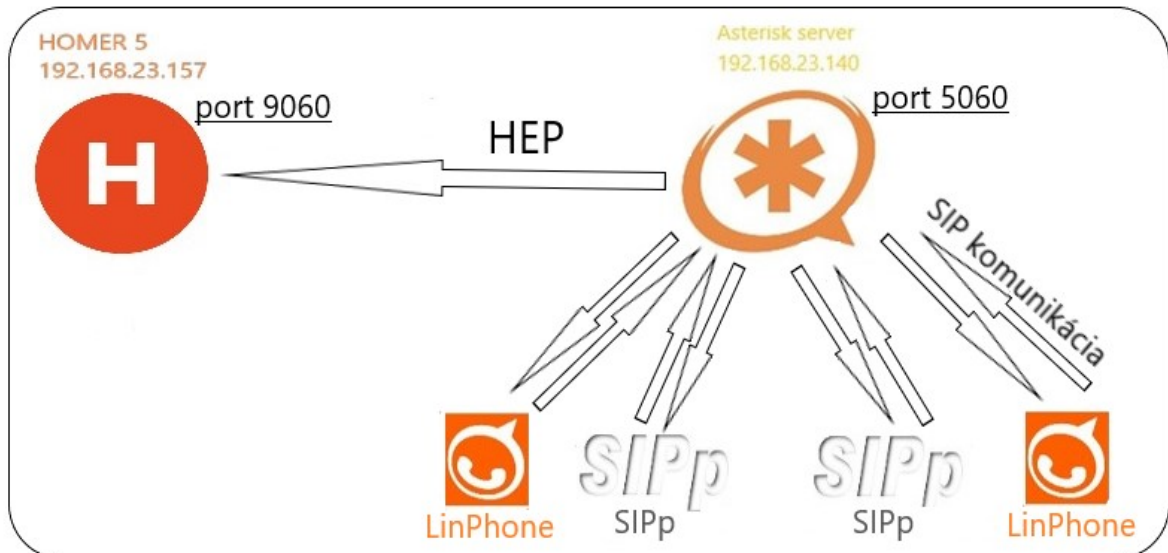
|                       |                 |
|-----------------------|-----------------|
| Incoming call created | 10              |
| Outgoing call created | 0               |
| Total Call created    | 10              |
| Successful call       | 10              |
| Failed call           | 0               |
| Call Length           | 00:00:14:016000 |
| Response Time 1       | 00:00:00:002000 |

Dôležitý faktor v tabuľkách 1.1 a 1.2 je práve kolonka úspešných hovorov. V mojom prípade všetko prebehlo bez problémov, takže SIPp mám pripravený k použitiu.

Týmto mám všetko potrebné pripravené k analýze dát.

## 7 Analýza dát

Testovacie prostredie a všetko potrebné mám pripravené, takže môžem začať s analýzou dát.



Obrázok: 2.7 Testovacie prostredie

Na Obrázku 2.7 môžeme vidieť moje testovacie prostredie, ktoré využijem k analýze a testovaniu.

Pre mňa je práve dôležitý testovací nástroj SIPp, VoIP telefóny LinPhone mi poslúžili len k otestovaniu funkčnosti mojej Asterisk PBX.

### 7.1 HOMER 5 - Analýza dát

HOMER 5 ponúka obrovské množstvo funkcií, ja začnem tou z môjho pohľadu najdôležitejšou a to SIP Search, teda vyhľadávanie.

Po prihlásení do užívateľského prostredia HOMER 5 klikneme na záložku **Panels -> SIP Search**, kde môžeme po stlačení na tlačidlo Search vidieť prehľadne vypísanú komunikáciu. Toto vyhľadávanie ponúka aj rozšírené možnosti vyhľadávania napríklad podľa zdrojovej/cielovej IP adresy.

SIP Signaling

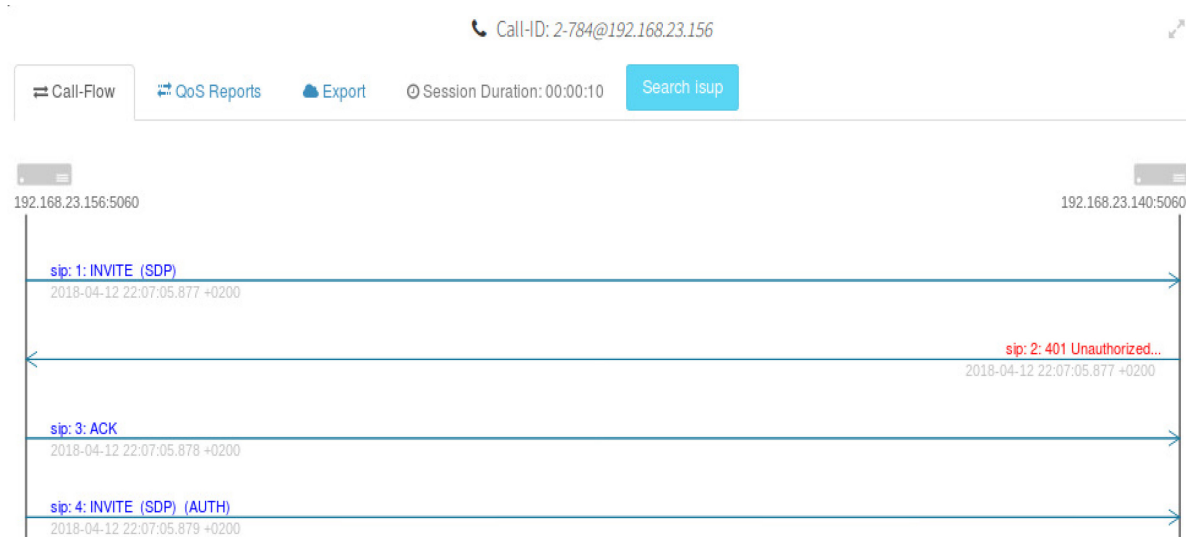
| ✓ | Id | Date                        | Method | Reason     | RURI user | From User | To User | CallID                  |
|---|----|-----------------------------|--------|------------|-----------|-----------|---------|-------------------------|
| ✓ | 6  | 2018-04-12 22:07:04.884 ... | 180    | Ringling   |           | 100       | 150     | 1-784@192.168.23.156    |
| ✓ | 7  | 2018-04-12 22:07:04.885 ... | 200    | OK         |           | 100       |         | d5ea44a9-a91e-4e3a-8... |
| ✓ | 8  | 2018-04-12 22:07:04.885 ... | ACK    |            |           | 100       |         | d5ea44a9-a91e-4e3a-8... |
| ✓ | 12 | 2018-04-12 22:07:04.886 ... | ACK    |            | 150       | 100       | 150     | 1-784@192.168.23.156    |
| ✓ | 11 | 2018-04-12 22:07:04.886 ... | 200    | OK         |           | 100       | 150     | 1-784@192.168.23.156    |
| ✓ | 14 | 2018-04-12 22:07:05.877 ... | INVITE |            | 151       | 101       | 151     | 2-784@192.168.23.156    |
| ✓ | 13 | 2018-04-12 22:07:05.877 ... | 401    | Unautho... |           | 101       | 151     | 2-784@192.168.23.156    |
| ✓ | 15 | 2018-04-12 22:07:05.878 ... | ACK    |            | 151       | 101       | 151     | 2-784@192.168.23.156    |
| ✓ | 16 | 2018-04-12 22:07:05.879 ... | INVITE |            | 151       | 101       | 151     | 2-784@192.168.23.156    |
| ✓ | 17 | 2018-04-12 22:07:05.880 ... | 100    | Trying     |           | 101       | 151     | 2-784@192.168.23.156    |
| ✓ | 18 | 2018-04-12 22:07:05.881 ... | INVITE |            |           | 101       |         | 71a72d6c-6829-467d-b... |
| ✓ | 20 | 2018-04-12 22:07:05.882 ... | 180    | Ringling   |           | 101       |         | 71a72d6c-6829-467d-b... |
| ✓ | 19 | 2018-04-12 22:07:05.882 ... | 180    | Ringling   |           | 101       | 151     | 2-784@192.168.23.156    |

Obrázok 2.8: SIP vyhľadavanie

Na Obrázku 2.8 môžeme vidieť prehľadne zobrazené jednotlivé hovory, ktoré su farebne rozlíšené a taktiež každý hovor má svoje unikátne CallID. Môžeme vyčítať, kto komu a kedy volal, ako dlho trval jednotlivý hovor, postupne rozpísané SIP žiadosti a odpovede daného hovoru.

Na podrobnejší rozbor som si vybral hovor s CallID 2-784@192.168.23.156.

Po kliknutí na priamo na CallID hovoru sa zobrazí rebríkový diagram, kde je podrobne zobrazená komunikácia hovoru.



Obrázok 2.9: Rebríkový diagram hovoru s CallID 2-784@192.168.23.156

Ako môžeme vidieť na Obrázku 2.9, v rebríkovom diagrame máme postupne rozpísané jednotlivé SIP žiadosti a odpovede. Ďalej tu nájdeme Session Duration, teda dobu trvania 10 sekúnd, túto dobu som si

nastavil v SIPp UAC príkaze, konkrétne je to -set duration 10000(ms), viz. pod kapitola 6.2. Dáta si ďalej môžeme uložiť kliknutím na Export do súborov .pcap, .txt, .png a ďalšie.

Ďalšou funkciou, ktorú SIP Search ponúka je možnosť priamo si otvoriť vybratú SIP požiadavku alebo odpoveď. Ja som si vybral správu INVITE.

MSG ID: 14

Message Details

2018-04-12 22:07:05 +0200 : 192.168.23.156:5060 -> 192.168.23.140:5060

**INVITE** sip:151@192.168.23.140 SIP/2.0  
Via: SIP/2.0/UDP 192.168.23.156:5060;branch=z9hG4bK-784-2-1  
From: <sip:101@192.168.23.140>;tag=784SIPpTag002  
To: <sip:151@192.168.23.140>  
Call-ID: 2-784@192.168.23.156  
CSeq: 1 **INVITE**  
Contact: <sip:101@192.168.23.156:5060>  
Max-Forwards: 70  
Subject: Performance Test  
Content-Type: application/sdp  
Content-Length: 161

v=0  
o=101 53655765 2353687637 IN IP4 192.168.23.156  
s=-  
c=IN IP4 192.168.23.156  
t=0 0  
m=audio 6004 RTP/AVP 8  
a=rtpmap:8 PCMA/8000  
a=ptime:20  
a=sendrecv

MSG ID: 14

Message Details

|             |                        |
|-------------|------------------------|
| id          | 14                     |
| date        | 2018-04-12 20:07:05    |
| milli_ts    | 1523563625677          |
| micro_ts    | 1523563625877000       |
| method      | INVITE                 |
| ruri        | sip:151@192.168.23.140 |
| ruri_user   | 151                    |
| ruri_domain | 192.168.23.140         |
| from_user   | 101                    |
| from_domain | 192.168.23.140         |
| from_tag    | 784SIPpTag002          |
| to_user     | 151                    |

Obrázok 3.0: Detaily SIP správy INVITE hovoru s CallID 2-784@192.168.23.156

Na Obrázku 3.0 môžeme vidieť podrobne vypísanú hlavičku správy INVITE aj s SDP (Session Description Protocol). Nachádzajú sa tu detaily, ako čas, IP adresy UAC a Asterisk, odkiaľ kam, teda od užívateľa 101 užívateľovi 151. Ďalej sa tu nachádzajú parametre SDP, viz kapitola 1.3.6.

Ďalšou užitočnou funkciou je záložka **Panels -> Stats: IP Network**.

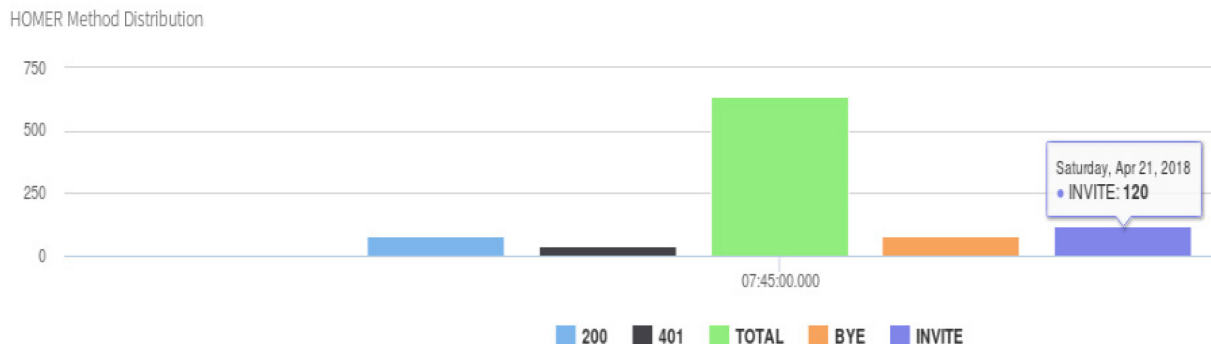
Tu sa nachádzajú grafy HOMER Method Distribution, HOMER Packet Count a SIPCapture Charts. Pre tento účel som s pomocou SIPp vykonal 4 testy, kde som menil počet hovorov -m.

Začal 5 hovormi, následne 10, 20 a potom znova 5.

Každý test som uskutočnil v rozmedzí 15 až 30 minút. Postupne sa mi v grafoch objavovali výsledky.

Prvý HOMER Method Distribution zobrazuje celkový počet SIP správ. Časové pásmo som si nastavil tak, aby sa mi zobrazovali výsledky zo všetkých 4 testov

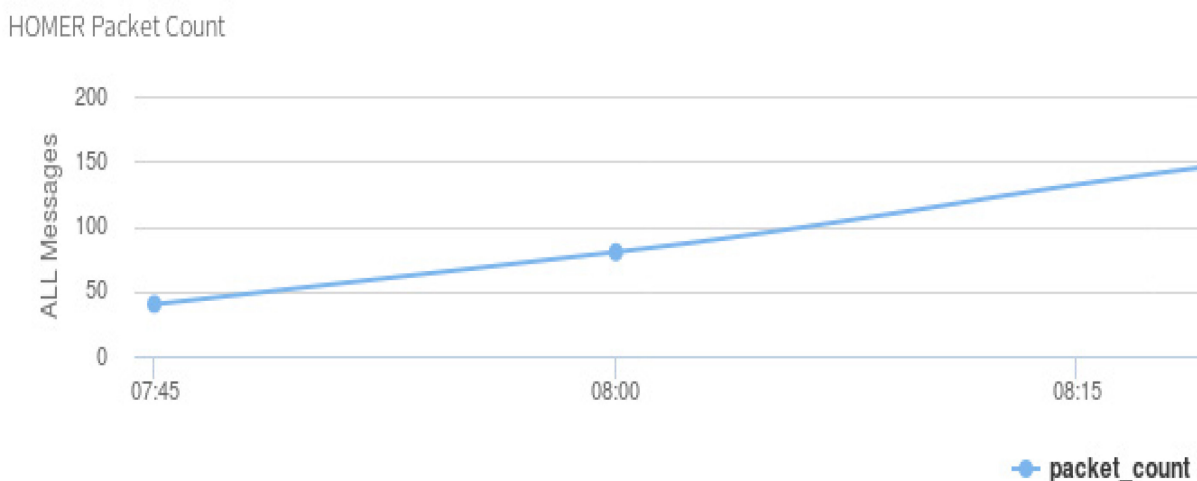




Obrázok 3.1: Štatistika jednotlivých SIP správ

Na Obrázku 3.1 môžeme vidieť štatistiky všetkých 4 testov, SIP správy a ich počty, ktoré sú prehľadne rozdelené.

HOMER Packet Count, ktorý zobrazuje počet paketov každého testu.

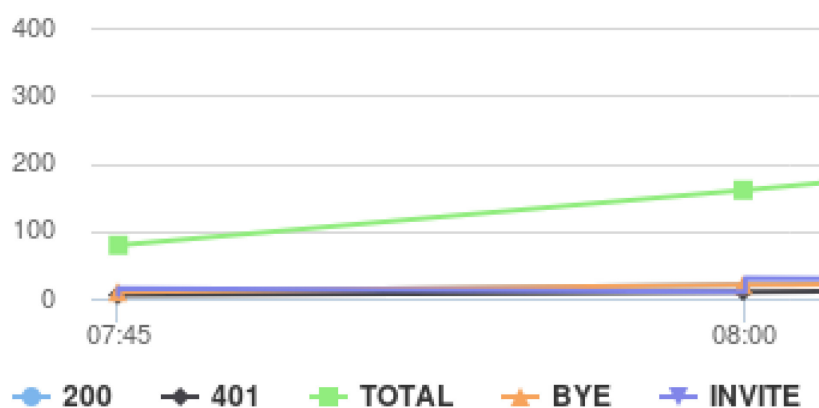


Obrázok 3.2: Počty paketov jednotlivých testov

Na Obrázku 3.2 môžeme vidieť, že prvý test som začal v čase 7:45, kde -m bolo 5 a celkový počet prenesených paketov je 40, v čase 8:00 som uskutočnil druhý test, kde -m bolo 10 a počet paketov sa zdvojnásobil na 80.

Posledným grafom je SIPCapture Charts, tento graf je podobný s HOMER Packet Distribution s tým, že tu tiež môžeme znova nájsť jednotlivé počty SIP správ, ale tie su už rozdelené medzi jednotlivé testy.

SIPCapture Charts



Obrázok 3.3: SIP štatistika jednotlivých testov

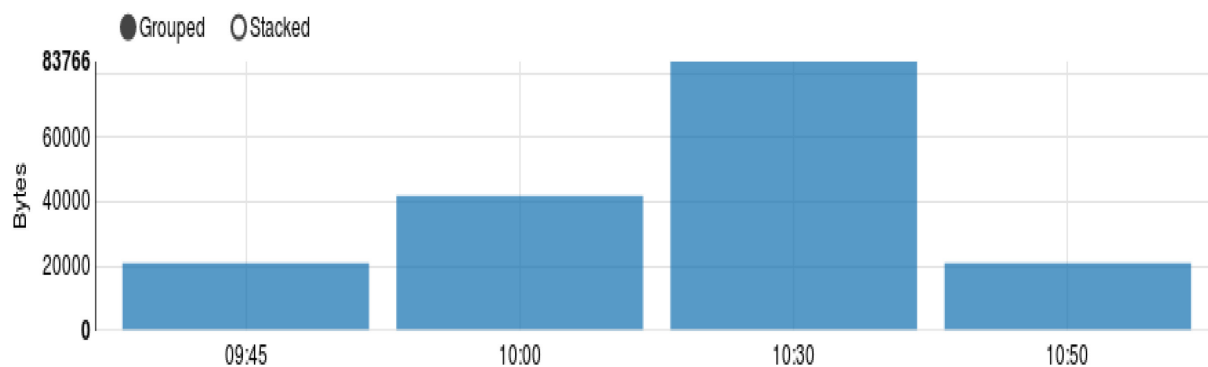
Na Obrázku 3.3 som si vybral rovnaké testy ako na Obrázku 3.2, tu vidíme graf týchto testov, čím viac hovorov som v danom teste uskutočnil, tým aj stúpali počty jednotlivých SIP správ.

Teraz sa môžem posunúť k ďalšej funkcii **Panels -> Stats: VoIP Traffic**

Zaujímavou štatistikou, ktorá sa tu nachádza je SIPCapture Packet Size HEP, čo je veľkosť HEP paketu, ktorý bol prenesený počas testu, jednotkou je Byte[B].

SIPCapture Packet Size HEP

2 -



Obrázok 3.4: Veľkosť HEP paketov jednotlivých testov

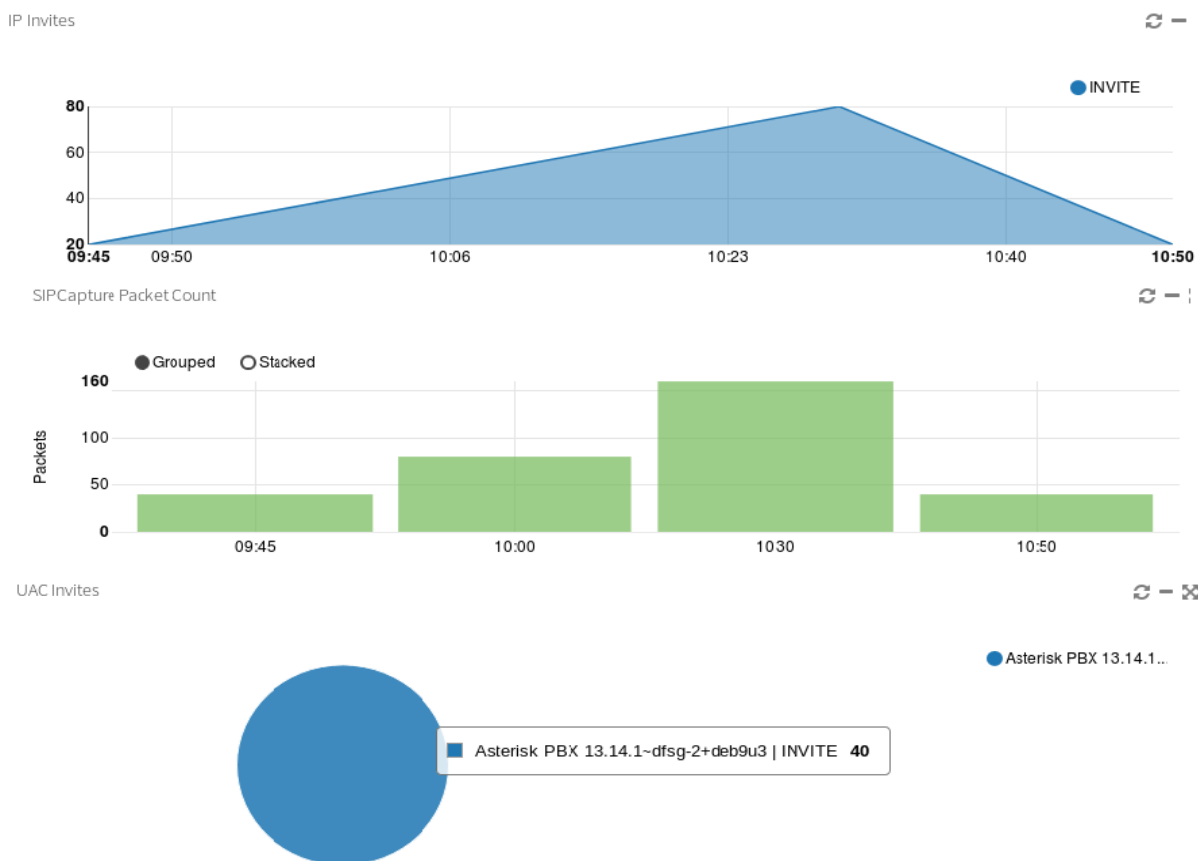
Na Obrázku 3.4 môžeme vidieť veľkosti HEP paketov jednotlivých testov.

Tabulka 1.3: *Velkosť jednotlivých HEP paketov*

| Čas   | Velkosť HEP paketu [B] | Počet hovorov -m |
|-------|------------------------|------------------|
| 9:45  | 20889                  | 5                |
| 10:00 | 41820                  | 10               |
| 10:30 | 83766                  | 20               |
| 10:50 | 20897                  | 5                |

Z tabulky 1.3 môžeme vyčítať, že zdvojnásobením počtu hovorov sa aj veľkosť HEP zdvojnásobí.

Ďalšími grafmi, ktoré sa tu nachádzajú je napríklad SIPCapture Packet Count, veľmi podobný grafu HOMER Packet Count, graf IP Invites a UAC Invites, ktorý zobrazuje počet správ z môjho Asterisk serveru.



Obrázok 3.5: Grafy IP Invites, SIPCapture Packet Count a UAC Invites

Na Obrázku 3.5 môžeme vidieť ako stúpali a klesali počty INVITE požiadavku alebo počet UAC Invite správ.

## 7.2 Overenie dôveryhodnosti získaných dát

Takže, vykonal som analýzu získaných dát a možnosti analýzy dát v systéme HOMER 5. V tejto kapitole sa budem venovať overeniu dôveryhodnosti získaných dát, to že nejaké dáta v HOMER 5 mám ešte neznamená, že sú zobrazované správne.

Ako overenie som zvolil porovnanie dát, ktoré sa zobrazujú v systéme HOMER 5 s dátami, ktoré si odchytiť a uložiť do súboru .pcap. K tomuto overeniu využijem nástroj Wireshark.

### 7.2.1 Porovnanie dát pomocou nástroja Wireshark

Ako prvé si musím odchytiť dáta, ktoré budem následne porovnávať. K tomuto mi posluží nástroj tcpdump. Tieto dáta si musím odchytiť priamo na Asterisk servery.

Do terminálu zadám príkaz:

- **tcpdump -nqt -s 0 -A -i ens33 port 5060 -w bak.pcap**

Pomocou tcpdump si odchytiť SIP prevádzku (port 5060) na rozhraní ens33 a uložiť ju do súboru bak.pcap. Nástroj tcpdump musíme spustiť pred začatím testovania, samozrejme ak chceme všetky potrebné dáta.

Týmto som získal dáta, ktoré budem porovnávať s dátami v systéme HOMER 5. Teraz môžem začať overovať dôveryhodnosť.

Tentokrát som zvolil -m 30, teda 30 hovorov. Po otvorení súboru .pcap vo Wireshark sa mi zobrazí priebeh jednotlivých hovorov a poradie SIP správ, ktoré môžem porovnať s dátami v HOMER. Vo Wireshark som klikol na záložku Telephony -> VoIP Calls, kde mám počet jednotlivých hovorov, je ich 30 a zhoduje sa mi so systémom HOMER.

Zvolil som hovor s CallID 3-24751@192.168.23.156

|     |                             |                        |                |          |  |     |  |
|-----|-----------------------------|------------------------|----------------|----------|--|-----|--|
| 669 | 2018-04-21 15:24:51.804 ... | <a href="#">INVITE</a> |                | 152      | 102  | 152 | <a href="#">3-24751@192.168.23.156</a> |
| 667 | 2018-04-21 15:24:51.804 ... | <a href="#">401</a>    | Unautho...     |          | 102  | 152 | <a href="#">3-24751@192.168.23.156</a> |
| 670 | 2018-04-21 15:24:51.805 ... | <a href="#">ACK</a>    |                | 152      | 102  | 152 | <a href="#">3-24751@192.168.23.156</a> |
| 665 | 2018-04-21 15:24:51.806 ... | <a href="#">INVITE</a> |                | 152      | 102  | 152 | <a href="#">3-24751@192.168.23.156</a> |
| 668 | 2018-04-21 15:24:51.807 ... | <a href="#">100</a>    | Trying         |          | 102  | 152 | <a href="#">3-24751@192.168.23.156</a> |
| 25  | 2.001189                    | 192.168.23.156         | 192.168.23.140 | SIP/S... | 577 Request: INVITE sip:152@192.168.23.140 |     |  |
| 26  | 2.001722                    | 192.168.23.140         | 192.168.23.156 | SIP      | 532 Status: 401 Unauthorized               |     |  |
| 27  | 2.002102                    | 192.168.23.156         | 192.168.23.140 | SIP      | 398 Request: ACK sip:152@192.168.23.140    |     |  |
| 28  | 2.003813                    | 192.168.23.156         | 192.168.23.140 | SIP/S... | 839 Request: INVITE sip:152@192.168.23.140 |     |  |
| 29  | 2.004607                    | 192.168.23.140         | 192.168.23.156 | SIP      | 358 Status: 100 Trving                     |     |  |

Obrázok 3.6: Porovnanie SIP správ v HOMER(hore) a Wireshark(dole)

Na Obrázku 3.6 môžeme vidieť, že jednotlivé správy sa zhodujú, čo naznačuje, že dáta sú zobrazované správne.

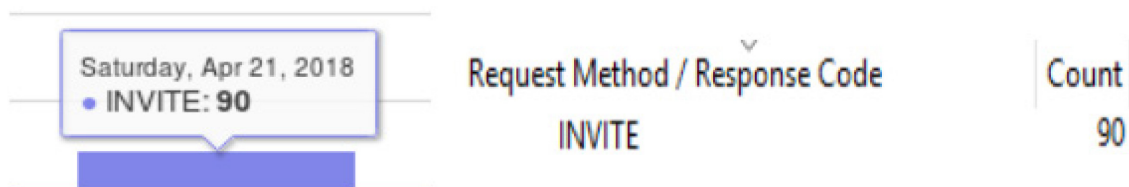
Ako ďalšie porovnanie na overenie dôveryhodnosti som zvolil porovnanie rebríkových diagramov zvoleného hovoru.



Ako môžeme vidieť na Obrázku 3.8, tak SIP hlavičky aj s SDP sa presne zhodujú. Či už sa pozrieme na polia VIA, FROM, TO, CallID, Contact, všetko je presne tak ako zobrazuje HOMER 5.

Týmto porovnaním si už môžem urobiť obraz o dôveryhodnosti dát, ktoré sa mi zobrazujú v mojom systéme. Zatiaľ sa všetko zhoduje.

Ďalej si môžem porovnať počet SIP správ. Na každý hovor pripadajú 3 INVITE správy, HOMER aj Wireshark zobrazujú 90 INVITE správ, čo je správne, nakoľko som mal 30 hovorov.



*Obrázok 3.9: Porovnaní počtu INVITE správ HOMER (vľavo) Wireshark(vpravo)*

Na Obrázku 3.9 môžeme vidieť počet jednotlivých INVITE správ, ktoré sa zhodujú. Pre zobrazenie som vybral graf HOMER Method Distribution, viz. Obrázok 3.1 a vo Wireshark záložka Telephony -> SIP Statistics.

Rovnako ako správy INVITE sa mi zhodovali aj počty ostatných SIP správ.

Týmto porovnaním si som overil dáta a môžem skonštatovať, že dáta, ktoré sa mi zobrazujú v mojom systéme HOMER 5, ktorý som nakonfiguroval sú správne a dôveryhodné.

## 8 Zátťažový test navrhnutého systému

Mojou ďalšou úlohou je vykonať záťažový test navrhnutého systému. Pri tomto teste som obmedzený výkonom svojho počítača, ale budem sa snažiť vykonať ho čo najpresnejšie.

V UAC príkaze SIPp budem meniť parametre a sledovať či všetky hovory boli alebo neboli úspešné. Hlavné parametre, ktoré budem meniť sú:

- **Počet hovorov -m**
- **Dĺžku hovoru -set call\_duration**
- **Ratio -r a ratio period -rp**

Príkazy sú podrobne rozpísané v podkapitole 6.2

Postupne budem sledovať, či sa objavia nejaké chyby. Testy pri ktorých nastanú nejaké chyby vykonám pre porovnanie s rovnakými parametrami 3 krát.

Tabulka 1.4: *Tabulka s výsledkami zo záťažového testu*

| -m  | -r  | -rp[s] | -set call_duration[ms] | Vytvorené hovory | Úspešné hovory | Neúspešné hovory |
|-----|-----|--------|------------------------|------------------|----------------|------------------|
| 10  | 1   | 1      | 5000                   | 10               | 10             | 0                |
| 10  | 5   | 1      | 10000                  | 10               | 10             | 0                |
| 10  | 10  | 0.5    | 5000                   | 10               | 10             | 0                |
| 50  | 1   | 1      | 5000                   | 50               | 50             | 0                |
| 50  | 25  | 1      | 10000                  | 50               | 50             | 0                |
| 50  | 50  | 0.5    | 5000                   | 50               | 49             | 1                |
|     |     |        |                        |                  | 42             | 8                |
|     |     |        |                        |                  | 37             | 13               |
| 100 | 1   | 1      | 5000                   | 100              | 100            | 0                |
| 100 | 50  | 1      | 10000                  | 100              | 100            | 0                |
| 100 | 100 | 0.5    | 5000                   | 100              | 79             | 21               |
|     |     |        |                        |                  | 65             | 35               |
|     |     |        |                        |                  | 90             | 10               |
| 200 | 1   | 1      | 5000                   | 200              | 200            | 0                |
| 200 | 100 | 1      | 10000                  | 200              | 190            | 10               |
|     |     |        |                        |                  | 193            | 7                |
|     |     |        |                        |                  | 199            | 1                |
|     |     |        |                        |                  | 133            | 67               |

|     |     |     |      |     |     |    |
|-----|-----|-----|------|-----|-----|----|
| 200 | 200 | 0.5 | 5000 | 200 | 118 | 82 |
|     |     |     |      |     | 141 | 59 |

Ako môžeme vidieť z výsledkov v Tabulke 1.4, systém je v rámci bežného používania veľmi stabilný. V prípade nastavenia jedného hovoru za 1 sekundu nenastala v žiadnom teste chyba.

Najväčšiu chybovosť môžeme vidieť pri nastavenom -r a -rp, tak aby boli všetky hovory prenesené za 2 alebo dokonca 0.5 sekundy. V týchto prípadoch má už Asterisk problémy tieto hovory úspešne zrealizovať.

Celkovo môžem zhodnotiť stabilitu systému ako veľmi dobrú, počas bežného testovania som neznamenal žiadne veľké problémy.



## Záver

Cieľom tejto bakalárskej práce bolo spojazdenie a zhodnotenie využiteľnosti systému HOMER 5, presnosti zobrazovaných dát, a aj rýchlosť aktualizácie prezentovaných dát.

V práci som sa venoval hlavne monitorovaciemu systému HOMER 5, jeho účelu, možnosti analýzy SIP signalizácie a prepojenie s ďalšími systémami. Cestu ako "nainštalovať" HOMER 5 som zvolil spustenie pomocou kontajnerovej platformy DOCKER. Následne som HOMER 5 prepojil so softwarovou ústredňou Asterisk, ktorú som si nainštaloval a nakonfiguroval pomocou PJSIP. O prenos signalizácie medzi HOMER 5 a Asterisk PBX sa staral HEP protokol, ktorý bol zodpovedný za doručenie paketov systému HOMER 5. Týmto som si splnil základ potrebný pre vytvorenie testovacieho prostredia.

Po nainštalovaní, spojazdnení a prepojení HOMER 5 a Asterisk PBX som si vytvoril testovacie prostredie, ktoré sa skladá z monitorovacieho nástroja HOMER 5, Asterisk PBX a koncových bodov vytvorených pomocou PJSIP, viz Obrázok. 2.7. Na začiatku som mal vytvorené len dva koncové body, ktoré mi poslúžili len ako test funkčnosti Asterisku a HOMER 5, konkrétne som pre test použil VoIP telefóny LinPhone. Po otestovaní funkčnosti som sa mohol pustiť do testovania samotného systému HOMER 5, kde som overoval jeho možnosti a dôveryhodnosť dát, ktoré zobrazuje.

K testom mi poslúžil testovací nástroj SIPp, ktorý slúži k testovaniu SIP protokolu. Zadefinoval som si ďalších 100 koncových bodov, 50 predstavovalo UAC a 50 UAS. Následne som pomocou príkazov v ktorých som menil rôzne parametre simuloval SIP komunikáciu, ktorá sa mi následne zobrazila v systéme HOMER 5. Pomocou takto získaných dát som začal popisovať jednotlivé funkcie, ktoré HOMER 5 ponúka, hlavne vyhľadávanie a bližšiu analýzu paketov.

Dôveryhodnosť dát, ktoré sa mi zobrazujú som si overil porovnaním, nástroj ktorý mi slúžil na porovnávanie bol Wireshark. Priamo na Asterisku som si pomocou nástroja tcpdump odchytil práve prebiehajúcu SIP komunikáciu, ktorú som následne porovnával so systémom HOMER 5. Po rôznych testoch, ktoré som vykonal môžem skonštatovať, že dáta sú dôveryhodné a že moj navrhutý systém pracuje správne.

Po overení dôveryhodnosti som ešte vykonal záťažový test môjho systému, kde som zisťoval jeho stabilitu. Uskutočnil som sériu testov pomocou nástroja SIPp, kde som v príkazoch menil rôzne parametre tak, aby som postupne zaťažoval navrhnutý systém. Z výsledkov môžem skonštatovať, že systém je stabilný, chyby nastávali až pri veľkom počte prenesených hovorov za sekundu, čo som aj očakával.

Myslím si, že systém HOMER 5 je veľmi použiteľný v praktickom nasadení, či už sa jedná o pracovné alebo domáce použitie za účelom napríklad štúdia. Celkovo boli prezentované výsledky po správnom nakonfigurovaní veľmi presné, nestretol som sa so žiadnym vážnym problémom. Jediným problémom, ktorý sa vyskytoval počas celej doby testovania bola rýchlosť aktualizácie prezentovaných dát. Doba, kedy sa začali výsledky kompletne zobrazovať v systéme HOMER 5 prekročovala 10 minút.

## Použitá literatura

- [1] 1. díl - Základy VoIP [online]. [cit. 2018-03-25]. Dostupné z:  
<https://www.joyce.cz/cz/voip-reseni/vse-o-voip-rady-tipy/1-dil-zaklady-voip/>
- [2] Úvod do VoIP [online]. [cit. 2018-03-25]. Dostupné z:  
[http://www.mldata.cz/uvoddovoip.htm#\\_Využití\\_IP\\_telefonie](http://www.mldata.cz/uvoddovoip.htm#_Využití_IP_telefonie)
- [3] HARTPENCE, Bruce. Packet guide to Voice over IP. Tokyo: O'Reilly, 2013. ISBN 1449339670.
- [4] RFC 3550. Dostupné z:  
<https://tools.ietf.org/html/rfc3550>
- [5] Pauli Vesterinen. User authentication in SIP. [online] [cit. 2018-03-25]  
Dostupné z: [http://www.tml.tkk.fi/Publications/C/22/papers/Vesterinen\\_final.pdf](http://www.tml.tkk.fi/Publications/C/22/papers/Vesterinen_final.pdf)
- [6] SIP - Session Initiation Protocol [online]. [cit. 2018-03-28]. Dostupné z:  
[https://www.tutorialspoint.com/session\\_initiation\\_protocol/session\\_initiation\\_protocol\\_tutorial.pdf](https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_tutorial.pdf)
- [7] SIP [online]. [cit. 2018-03-28].  
Dostupné z: <https://sip.cesnet.cz/cs/protokoly/sip>
- [8] RFC 4566. Dostupné z:  
<https://tools.ietf.org/html/rfc4566>
- [9] Asterisk 13: stabilní motor pro vaše komunikace [online]. [cit. 2018-03-29]. Dostupné z:  
<https://www.root.cz/clanky/asterisk-13-stabilni-motor-pro-vase-komunikace/>
- [10] BRYANT, Russell. Asterisk: the definitive guide. Fourth edition. Sebastopol: O'Reilly, 2013. ISBN 978-1-449-33242-6.
- [11] Asterisk: VoIP ústředna - 2 (konfigurace) [online]. [cit. 2018-04-3]. Dostupné z:  
[https://data.kemt.fei.tuke.sk/KomunikacnaTechnika1/prednasky/26\\_9\\_2016/ST\\_ASTERISK\\_3\\_12\\_2013/Asterisk/ASTERISK/Asterisk\\_%20VoIP%20ústředna%20-%2020\(konfigurace\).pdf](https://data.kemt.fei.tuke.sk/KomunikacnaTechnika1/prednasky/26_9_2016/ST_ASTERISK_3_12_2013/Asterisk/ASTERISK/Asterisk_%20VoIP%20ústředna%20-%2020(konfigurace).pdf)
- [12] PJSIP [online]. [cit. 2018-04-3]. Dostupné z:  
<http://www.pjsip.org>
- [13] HOMER5 [online]. [cit. 2018-04-10]. Dostupné z:  
<https://github.com/sipcapture/homer>
- [14] SIPCATURE [online]. [cit. 2018-04-10]. Dostupné z:  
<https://www.kamailio.org/events/2016-KamailioWorld/Day2/17-Alexandr.Dubovikov-VoIP-RTC-Monitoring-Using-Sipcapture-HEP-Stack.pdf>

- [15] Začínáme s Dockerem na Fedore [online]. [cit. 2018-04-10]. Dostupné z:  
<https://mojefedora.cz/zaciname-s-dockerem-na-fedore/>
- [16] SIPp [online]. [cit. 2018-04-10]. Dostupné z:  
<http://sipp.sourceforge.net/doc/reference.pdf>
- [17] PJSIP Sections and Relationships [online]. [cit. 2018-04-12]. Dostupné z:  
<https://wiki.asterisk.org/wiki/display/AST/PJSIP+Configuration+Sections+and+Relationships>
- [18] Migrating from chan\_sip to res\_pjsip [online] [cit. 2018-04-15]. Dostupné z:  
[https://wiki.asterisk.org/wiki/display/AST/Migrating+from+chan\\_sip+to+res\\_pjsip](https://wiki.asterisk.org/wiki/display/AST/Migrating+from+chan_sip+to+res_pjsip)
- [19] Creating Dialplan Extensions [online]. [cit. 2018-04-15]. Dostupné z:  
<https://wiki.asterisk.org/wiki/display/AST/Creating+Dialplan+Extensions>
- [20] LinPhone [online]. [cit. 2018-04-15]. Dostupné z:  
<http://www.linphone.org/about.html>
- [21] Get Docker CE for Ubuntu [online]. [cit. 2018-04-15]. Dostupné z:  
<https://docs.docker.com/install/linux/docker-ce/ubuntu/>
- [22] SIPp [online]. [cit. 2018-04-15]. Dostupné z:  
<http://sipp.sourceforge.net/doc3.3/reference.pdf>

## **Zoznam príloh**

### **Elektronické prílohy**

Príloha I: Konfigurácia PC a Virtualizačná platforma.....- DVD -